

CHAPTER 2

Managing and Controlling Microsoft Teams

Balu N Ilag^a, Durgesh Tripathy

^a Tracy, CA, USA

As a Microsoft Teams administrator, you play a pivotal role in setting up, managing, and optimizing the collaborative environment within your organization. This chapter provides an overview of the various policies and functionalities you can control, ensuring smooth collaboration, data security, and user-friendliness. Managing and administering the Microsoft Teams experience involves overseeing a variety of tasks and functionalities to ensure a smooth, secure, and efficient collaborative environment for users within your organization.

We'll cover the following in this chapter:

- **Microsoft Teams Authentication process:** We'll cover how Microsoft Teams user authentication works and the Microsoft Teams sign-in process.
- **Teams and channels:** We'll cover how to deploy and manage teams and channels and how to manage the Teams desktop client.
- **Live events and Streams:** We'll show how to configure and manage live events and Microsoft Stream.
- **Administrative tools:** We'll show how to manage Teams using the Microsoft Teams admin center.
- **Messaging policies:** As an administrator, you can create and modify messaging policies that govern chat behaviors and options. This includes settings such as read receipts, URL previews, editing and deletion permissions, and GIF settings, among others.

- **Teams policies for channel creation and discovery:** Admins design policies to manage team creation and set up parameters that influence who can create teams, the naming conventions used, and how teams can be discovered by users.
- **Organization-wide settings for Teams:** These settings affect all teams within the organization, impacting features such as guest access, Teams for Education settings, and Teams Live events.
- **Private channel creation management:** Administrators manage who can create private channels, allowing for controlled, private collaboration within Teams without creating entirely new teams.
- **Email integration control:** Admins can enable or disable the ability to send emails to a channel in Teams, providing another way for users to share information.
- **File-sharing functions:** You can control the file-sharing functions from the Teams client, such as cloud storage options and the use of third-party storage providers.
- **Channel moderation setup:** Admins can set up channel moderation in Teams to control who can start new posts and control whether team members can reply.
- **Understanding the Teams admin center:** The Teams admin center is the primary portal for managing and configuring Teams; it provides tools for managing the entire life cycle of Teams from creation to archiving.
- **Additional tools:** We'll also cover Microsoft Azure Active Directory Center, the Microsoft 365 admin center, and the Microsoft 365 Security and Compliance Centers.
- **Teams management through PowerShell:** We'll also cover PowerShell in this chapter.

As a Teams administrator, understanding these tools and policies will enable you to create an environment that fosters collaboration, respects user needs, and aligns with organizational policies and compliance requirements. This knowledge is crucial to leverage the full potential of Microsoft Teams, driving efficiency and productivity within your organization.

Microsoft Teams Authentication

How does Microsoft Teams user authentication work? Microsoft Teams uses Azure AD as the identity service to authenticate Teams users. Azure AD is purely a cloud-based identity and access management service for Office 365, but that doesn't mean you cannot use the on-premises Active Directory Domain Service (ADDS) identity service. You as an admin need to synchronize your on-premises user identities to Azure AD so that the user identities will be available in the Azure AD cloud, and then it will authenticate users using their user principal name (UPN) and password. For example, my UPN is `balu@cyclotron.com`, and I can sign into Teams using my password.

Azure AD is a crucial part of the overall deployment of Teams and how it works. The million-dollar question is, what is Azure AD, and how does Teams leverage it?

As mentioned, Azure AD is the cloud-based identity and access management service for Microsoft Office 365 services. Microsoft Teams leverages identities stored in Azure AD for collaboration and communication purposes. From a license requirements standpoint, Teams and Azure AD are included in a large number of licensing bundles, including small business plans like Office 365 Business; enterprise plans like Microsoft 365 Enterprise E1, E3, and E5; education plans like Office 365 Education; and developer plans like Office 365 Developer.

Another critical question is, how do I manage cloud identity with Azure AD? Because Teams is a cloud-only service and highly dependent on Azure AD, as a Teams admin you must know how cloud identity is managed in your Teams deployments and specifically how Teams credentials are managed and securely stored. Azure AD provides managed identities, which offers access to Azure and Office 365 resources for custom applications and services including Teams. The facility provides Azure services with an automatically managed identity in Azure AD. You can use this identity to authenticate to any service that supports Azure AD authentication, such as Teams, Exchange Online, SharePoint, OneDrive, and Yammer.

Now that you know the importance of Azure AD, how do you make sure the access permissions that users have are protected? Because Azure AD allows users to collaborate with internal users (within the organization) as well as external users (users outside the organization, like vendors or partners), it's crucial that you as an admin regularly review users' access to ensure that only the right people have access to cloud resources. This can be achieved through an Azure AD feature called *access reviews*, which enables organizations to effectively manage group memberships, access to enterprise applications, and role assignments.

Note Using the Azure AD access review feature requires an Azure AD Premium P2 license.

Microsoft Teams Sign-in Process

Microsoft Teams, like other Microsoft 365 services, uses Azure AD for authentication. As mentioned, Azure AD is Microsoft’s cloud-based identity and access management service. Microsoft Teams leverages Azure AD for authentication, and it uses Modern Authentication for sign-in and to protect login credentials. What is Modern Authentication, and why does Teams use it? It allows Teams apps to understand that users have previously registered and logged in with their credentials (like their work or institutional email and password) somewhere else, so they are not required to enter credentials again to initiate the Teams app.

Remember, Teams has clients for Windows, macOS, iOS, Linux, and Android, so the user experience might be different for each client platform. Another reason for the experience variation is the authentication method that an organization chooses. Usually there are two authentication methods: single-factor authentication (based on the user account and password) and multifactor authentication (involving more than one factor, such as verification over the phone or with a PIN along with a user account and password). The user experience will differ depending on the authentication method.

As a Teams admin, you must understand the different login experiences for Windows and Mac users.

Figure 2-1 shows a logical representation of the sign-in process with a call flow.

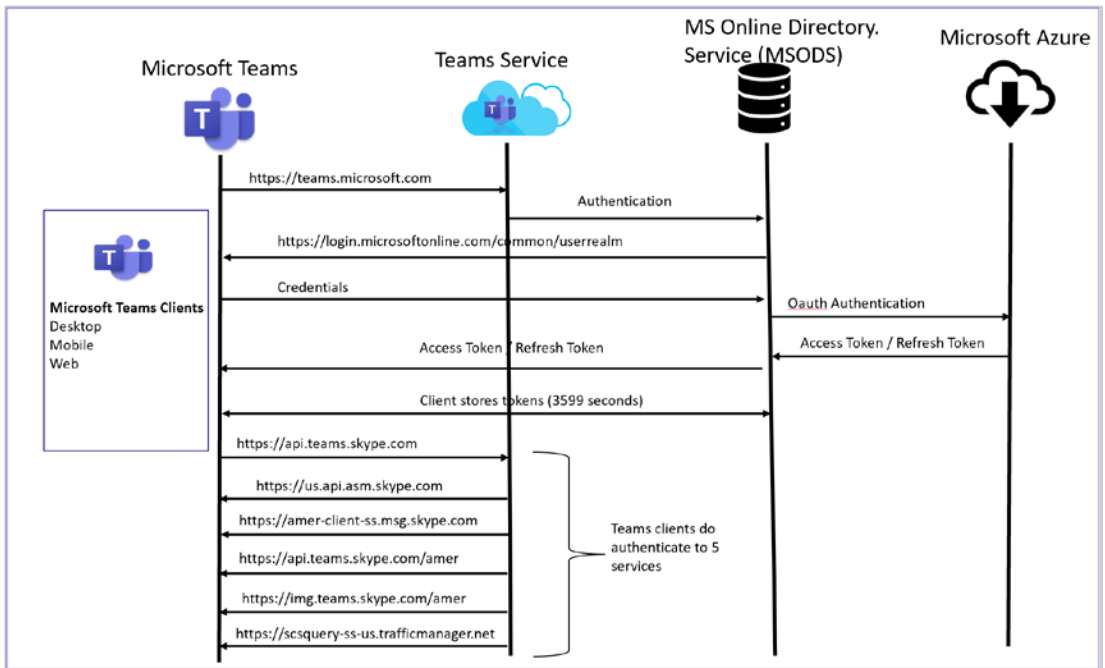


Figure 2-1. Teams client sign-in process

Here's a simplified explanation of the sign-in process:

1. **User sign-in:** When a user tries to sign into Microsoft Teams, the application directs the user to Azure AD for sign-in. The user enters their username and password in the sign-in page hosted by Azure AD.
2. **Authentication:** Azure AD verifies the user's credentials against the stored user information. If multifactor authentication (MFA) is enabled for the user's account, Azure AD will also prompt for additional verification, such as a phone call, text message, or mobile app notification.
3. **Authorization:** If the user's credentials are correct, Azure AD issues a security token, known as an *access token*, back to the Teams application. This token contains information about the user's identity, the application, and permissions or scopes.
4. **Access:** The Teams application uses this access token to authorize the user and grant them access to the service.

5. **Session:** The user is now signed into Teams and can begin interacting with the application. Their session will remain active until they sign out or until their access token expires, at which point they may need to re-authenticate.

For additional security, Teams also supports conditional access policies. For instance, organizations can set up policies to require MFA when users are signing in from unfamiliar locations or block sign-ins from specific regions or IP addresses. Remember, this content is current as of the time of writing (late 2023). For the most recent information, you should refer to Microsoft’s official documentation or contact Microsoft directly.

Using the Teams Client on macOS

When users use Teams on macOS, their Teams client cannot pull the credentials from their Office 365 enterprise account or any of their other Office applications. As an alternative, they will get a credential prompt asking them to enter a single-factor authentication (SFA) or MFA credential based their organization setting. As soon as they enter the required credential, Teams will sign them in, and they won’t have to enter their credential again. Instead, Teams will allow them to automatically sign in on the same macOS desktop.

Using Teams on a Windows Machine

When users are using Teams on a Windows desktop, their Teams client will be able pull the credentials from their Office 365 enterprise account or any of their other Office applications (where they are already logged in), so users are not required to enter their credentials. If a user is not signed on to their Office 365 enterprise account anywhere else, when they start Teams, they are asked to provide either SFA or MFA, depending on what their organization requires.

Specific to the Windows Teams client, when users using their domain-joined desktop log in to Teams, they might be asked to go through an additional authentication prompt depending on whether their organization has chosen to require MFA or their desktop already requires MFA to sign in. If their desktop has previously required MFA to sign in, then users will automatically be signed into Teams as soon as it opens.

Note If a user signs out (by clicking their avatar at the top of the app and then signing out) from the Teams app after completing the Modern Authentication process, to log in again, they need to enter their login credentials to start the Teams app.

Keep in mind that Modern Authentication is offered for each organization that uses Microsoft Teams, so if users are unable to complete the login process, there could be a problem with their Microsoft 365 tenant, domain, or enterprise account. If federation is used, for example, authentication happens with a client on-premises AD via secure AUTH, ping, or OKTA (these are the third-party identity providers).

Step-by-Step Teams Client Login Process

Here is the login process:

1. First, the user enters a login credential in the Teams client, and the application directs the user to Azure AD for sign-in. The user enters their username and password on the sign-in page hosted by Azure AD.
2. The Teams client resolves the DNS record to `teams.microsoft.com`. Once it resolves, the Teams client connects to Teams services.
 - A. **Name:** `s-0005.s-msedge.net`
 - B. **Addresses:** `2620:1ec:42::132`, `52.113.194.132`
 - C. **Aliases:** `teams.microsoft.com`, `teams.office.com`, `teams-mira-afd.trafficmanager.net` and `teams-office-com.s-0005.s-msedge.net`
3. Teams services redirect the Teams client to Azure AD to get a token from Azure AD. If the user's credentials are correct, Azure AD issues a security token, known as an *access token*, to the Teams application. This token contains information about the user's identity, the application, and permissions or scopes.

4. Azure AD gives the client access token to the Teams application. Then the Teams application uses this access token to authorize the user and grant them access to the service.
5. The Teams client gives the access token to the Teams cloud service.
6. The Teams user is logged in to Teams services. The user is now signed in to Teams and can begin interacting with the application. Their session will remain active until they sign out or until their access token expires, at which point they may need to re-authenticate.

Managing and Configuring MFA and Conditional Access for Teams

What is conditional access in authentication? Azure AD conditional access is a Microsoft security feature that helps you control and secure access to your cloud apps, based on specific conditions from a central location. It is essentially an “if-then” policy execution framework for access control. When a user tries to access a resource, conditional access policies are evaluated to determine whether the request is allowed, is denied, or requires additional authentication steps.

As you learned, Microsoft Teams leverages Azure AD for authentication, and there are two different kinds of authentication: SFA and MFA. However, an organization can consider securing the authentication by allowing Teams access through specific conditions such as the use of a specific operating system or version, client version, network subnet, and so on. That’s where conditional access policies come in handy. Fundamentally, a conditional access policy is a set of regulations for access control based on several specifications such as client version, service, registration procedure, location, compliance status, and so on. Conditional access is used to decide whether the user’s access to the organization’s data is allowed. By using conditional access policies, you as an admin can apply the right access controls when needed to both keep your organization secure and allow users to access applications.

Here's a simple explanation of how Azure AD conditional access works:

- **Conditions:** These are the circumstances under which the policy applies. Conditions can include user or group membership, IP location information, whether the device is marked as compliant or not, and the perceived risk level of the sign-in attempt, among others.
- **Assignments:** After defining the conditions, the administrator assigns what should happen if these conditions are met. This involves defining users and groups, cloud apps, and conditions such as sign-in risk levels, device platforms, and more.
- **Access controls:** If the conditions are met, then certain controls are applied that are defined under access controls. Controls can either allow access, require additional authentication challenges (such as multifactor authentication), limit access, or even block access entirely.

For instance, you might set a policy that requires users to authenticate via MFA if they are trying to access sensitive resources and are not on the corporate network. This dynamic, risk-based approach to access control helps to secure your organization's resources while ensuring that valid users can stay productive and don't get locked out of their work.

Note Conditional access policies are applicable to all Microsoft Modern Authentication-enabled applications including Teams, Exchange Online, and SharePoint Online.

How Conditional Access Flow Works

Azure AD conditional access allows users to work from anywhere securely through condition-based access. It allows IT admins to define access rules based on their organizational requirements to allow access for applications through different

conditions. It is designed to enforce access policies based on specific conditions when users attempt to access applications such as Microsoft Teams. Here's how it might look for Teams:

1. **Access request:** A user tries to access Microsoft Teams, through the desktop app, web app, or mobile app.
2. **Authentication:** The user authenticates themselves via Azure AD. This could be via username and password, MFA, biometric data, or other means.
3. **Policy evaluation:** Once the user is authenticated, Azure AD checks all conditional access policies applicable to the user. It assesses the user's role, location, device status, sign-in risk, etc., and checks them against the conditions set in the policies.
4. **Enforce requirements:** If the user and their context meet the conditions of a policy, Azure AD then checks whether the user fulfils the requirements of that policy. For example, the policy may require the user to use a device that is compliant with company policies, complete MFA, or connect from a trusted network.
5. **Access decision:** Azure AD then makes a decision to either grant or deny access based on the requirements of the policy. The access can be granted fully, granted with limitations (like read-only access), or completely denied.
6. **Access to Teams:** If Azure AD grants access, the user can access Microsoft Teams with the level of access granted by the policy (e.g., full or limited). If access is denied, the user cannot access Teams.

This flow ensures that access to Microsoft Teams is granted in a secure manner, only under conditions that align with the organization's security policies. It provides a balance between security and productivity by enforcing security requirements without hindering user access to the tools they need for their work. Figure 2-2 shows signals on the right side: the access condition based on user and locations, device used with

version, application used with app version, and real-time risk. The access attempt gets verified, and based on the signals, the access attempt is allowed or MFA is required for a blocked access attempt. If access is allowed, the user connects their application client to the back-end service.

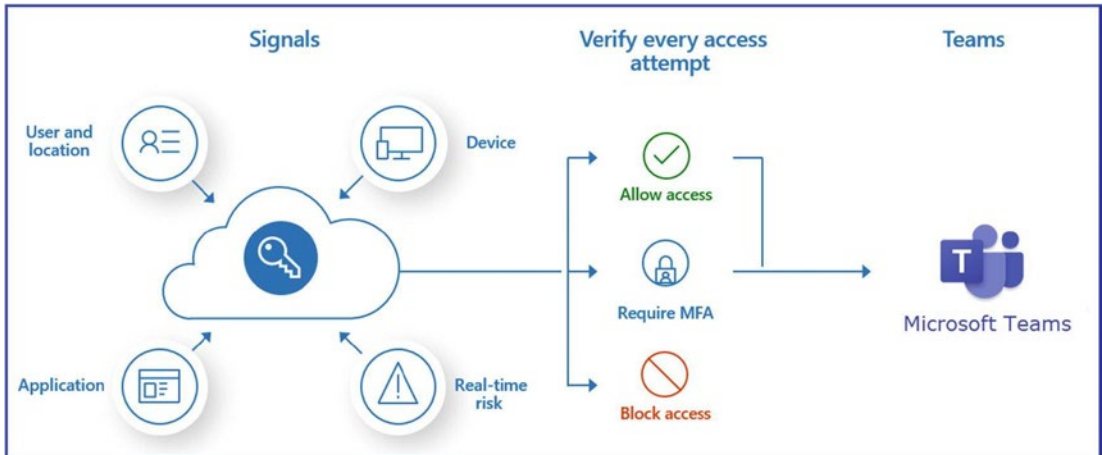


Figure 2-2. Azure AD conditional access

Managing Teams and Channels

In Chapter 1 you learned about teams and channels and their structure, as well as how to create organization-wide teams. We will now address how to manage teams and channels.

Before undertaking team management, you should understand how to create teams and channels effectively. To create a team, log in to Microsoft Teams and follow these steps:

1. Open the Teams app, log in, and click Teams, as shown in Figure 2-3. Then select “Join or create a team.”

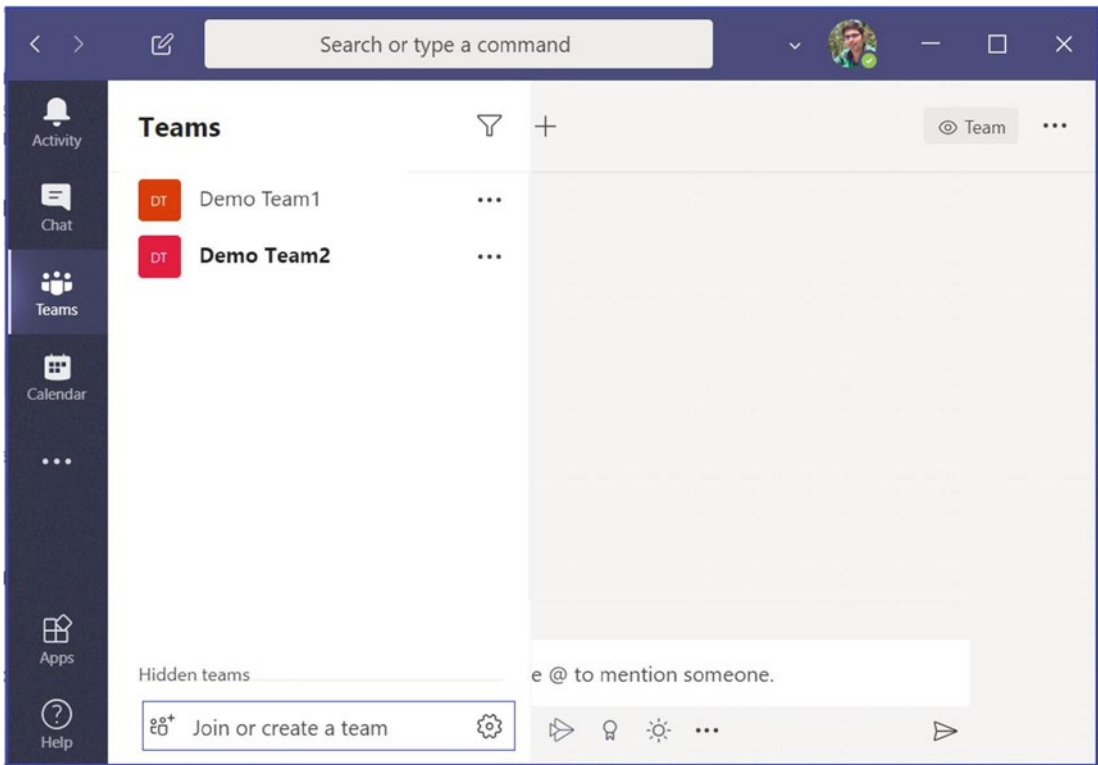


Figure 2-3. *Creating or joining teams*

2. Once the “Join or create team” page opens, click “Create team,” as shown in Figure 2-4.

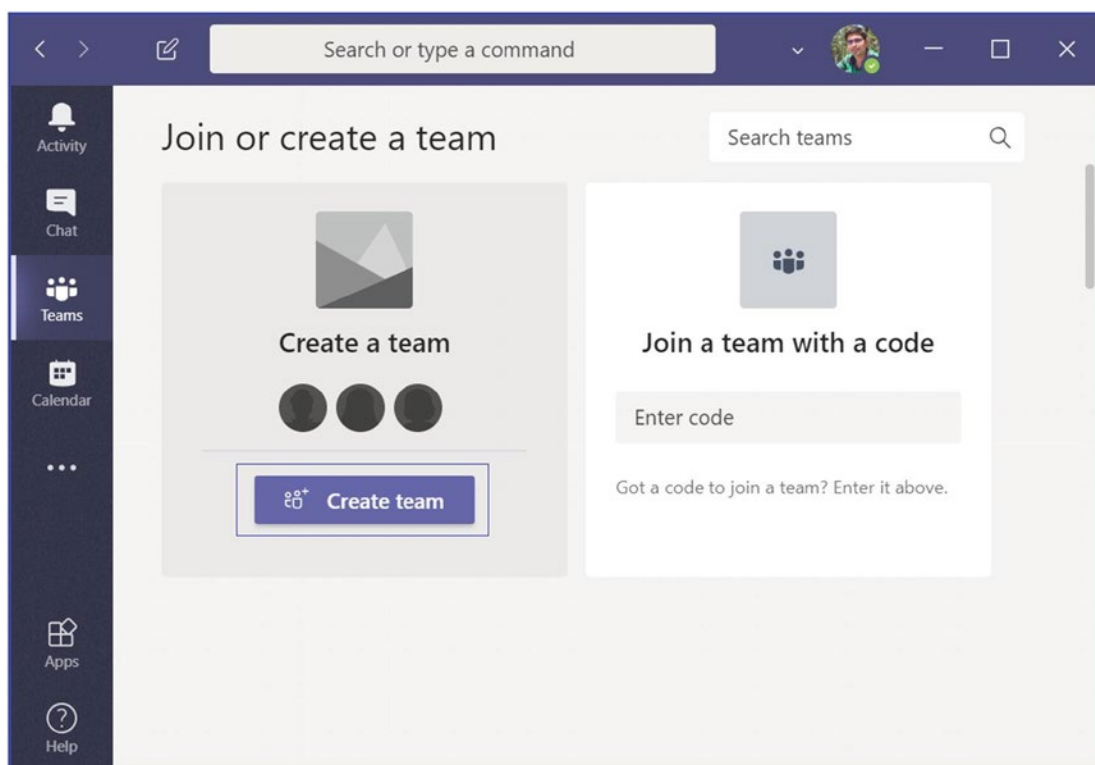


Figure 2-4. *Create team button*

3. Once you click “Create team,” it will display options to create a team from scratch or create a team using an existing Office 365 group. In Figure 2-5, we’re building a team from scratch.

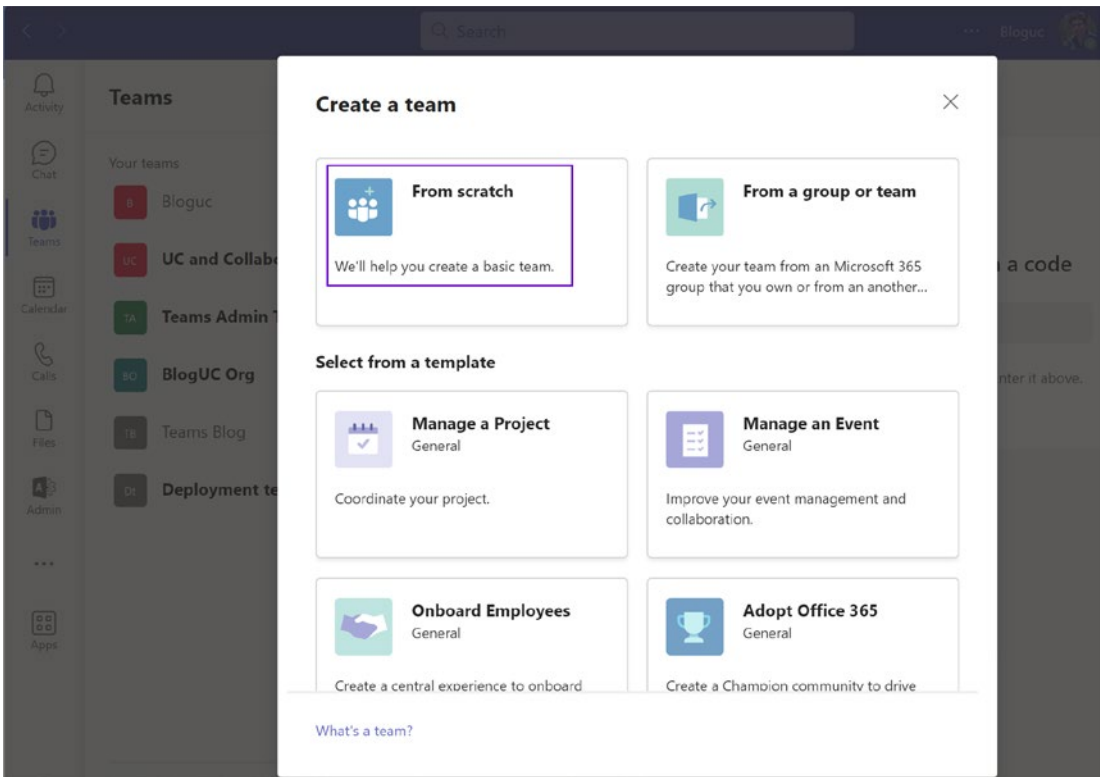


Figure 2-5. *Selecting an option to create a team from scratch or using an existing Office 365 group*

4. After selecting “From scratch,” you will be asked to choose what kind of team you will create, private or public. Remember for private teams, users need permission to join; for public teams, anyone in the organization can join without team owner permission. Figure 2-6 shows the selection of a private team.

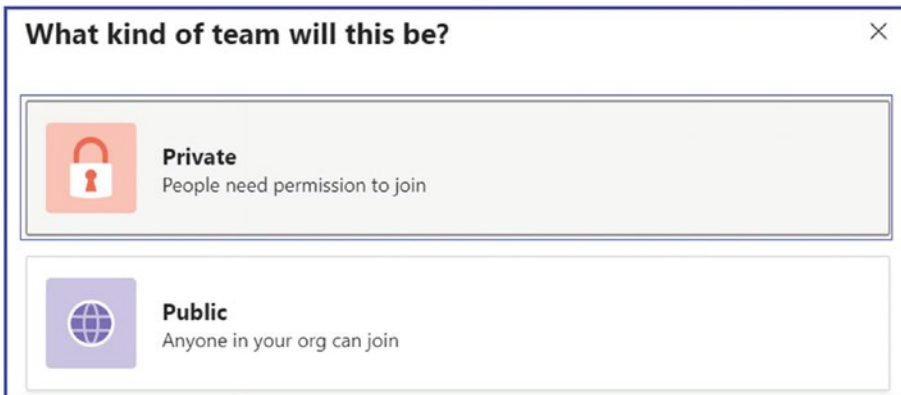


Figure 2-6. *The team type can be private or public*

- Next, provide an appropriate name and description for your team. Figure 2-7 shows the name Teams Administration Book Revision project and an appropriate description. Click Create; Teams will take some time to create the new team. Remember, creating a team means it will also create an Office 365 group, SharePoint Team site, and Exchange mailbox. Provisioning all these requires some time.

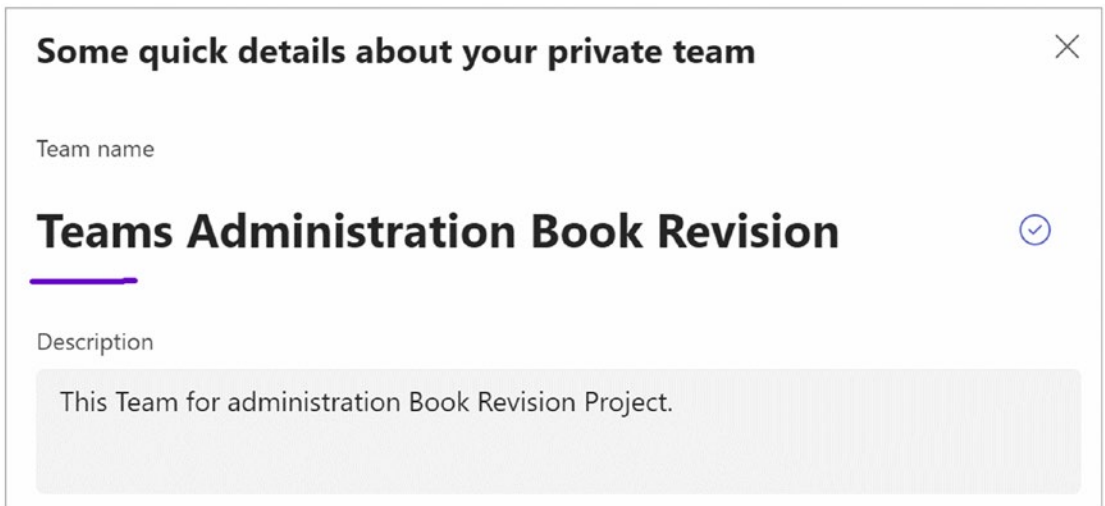


Figure 2-7. *Team name and description*

6. Next, add members to your team after team creation. Once you add the members, click Close to exit the member-adding window.

Figure 2-8 shows the added member Balu Ilag.

Note You can add a member by typing their name or adding a distribution list.

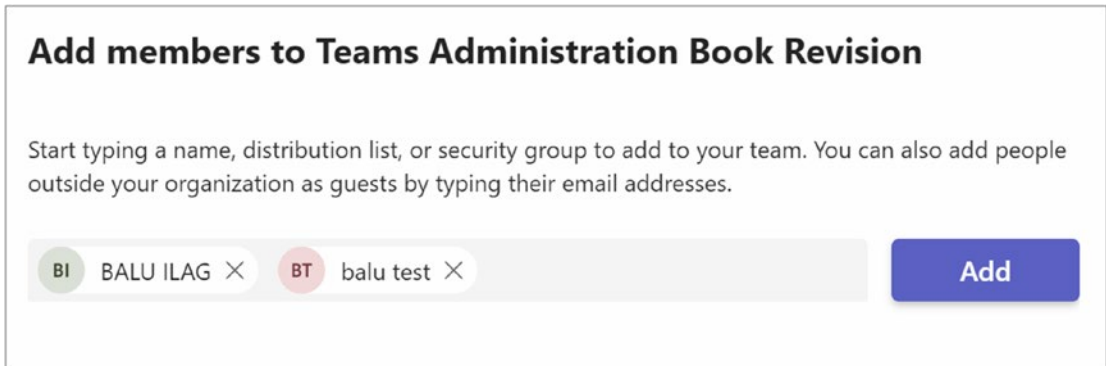


Figure 2-8. Adding a team member

7. Now you will can see that the team has been created, and a default channel was also added, called General. Figure 2-9 shows a team named Teams Administration Book Revision with the General channel.

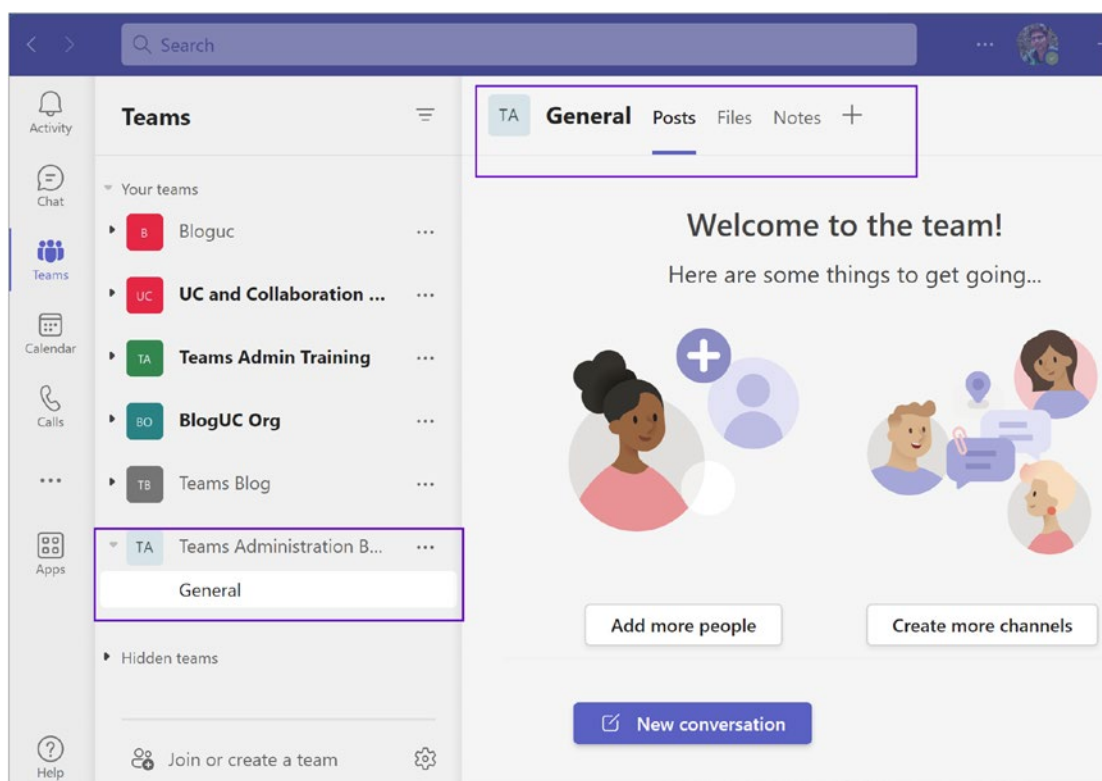


Figure 2-9. Team created with General channel

Note Creating a new team will automatically create a General channel that you cannot disable or delete.

Creating a Channel in a Team

Creating a team and channels in Microsoft Teams is a relatively simple process. Here's how you do it:

1. Navigate to the team for which you want to create a new channel and then click the three dots next to the team name.

2. From that list, select “Add channel” to create a channel, as shown in Figure 2-10.

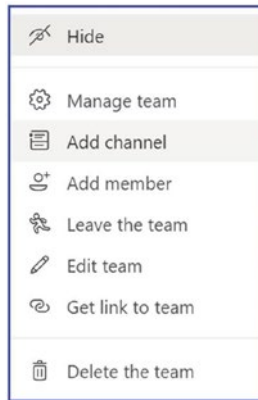


Figure 2-10. Adding a channel

3. You will see new windows where you can give a meaningful name and description to the channel, as well as select a privacy mode for the channel. Figure 2-11 shows the Standard channel privacy type selected. Remember, there are two privacy modes.
 - *Standard channel:* This privacy mode allows anyone (team members) to access this channel’s content within the team. These channels are open and available to all members of the team. They are best for topics that everyone in the team needs to see. For example, in a team dedicated to a project, there might be standard channels for Design, Development, Marketing, etc.
 - *Private channel:* A private channel is a subset of a team and can be accessed only by certain members of the team. Private channels are useful for sensitive discussions or when a project or topic involves a subgroup of the larger team. For example, in a team dedicated to a project, there might be a private channel called Project Leaders, where only the leadership team can access and discuss higher-level strategies.

- *Shared channel:* Microsoft Teams' shared channels offer spaces where collaboration can take place with individuals who may not belong to the same team. Access to these channels is limited to those who have been designated as owners or members. Although individuals with guest status in your organization's Azure Active Directory cannot be included in a shared channel, Azure AD B2B Direct Connect provides a mechanism for inviting people outside your organization to participate in a shared channel.

Create a channel for "Teams Administration Book Revision" team

Channel name
Chapter1

Description (optional)
Help others find the right channel by providing a description

Privacy
Standard - Everyone on the team has access

Automatically show this channel in everyone's channel list

Cancel Add

Figure 2-11. *Creating a channel and selecting a privacy mode*

Click Add to create the channel. Figure 2-12 shows the newly created channel and default features available to use. After channel creation, it will show the Posts and Files wiki tabs. You can add additional tabs by clicking the plus sign.

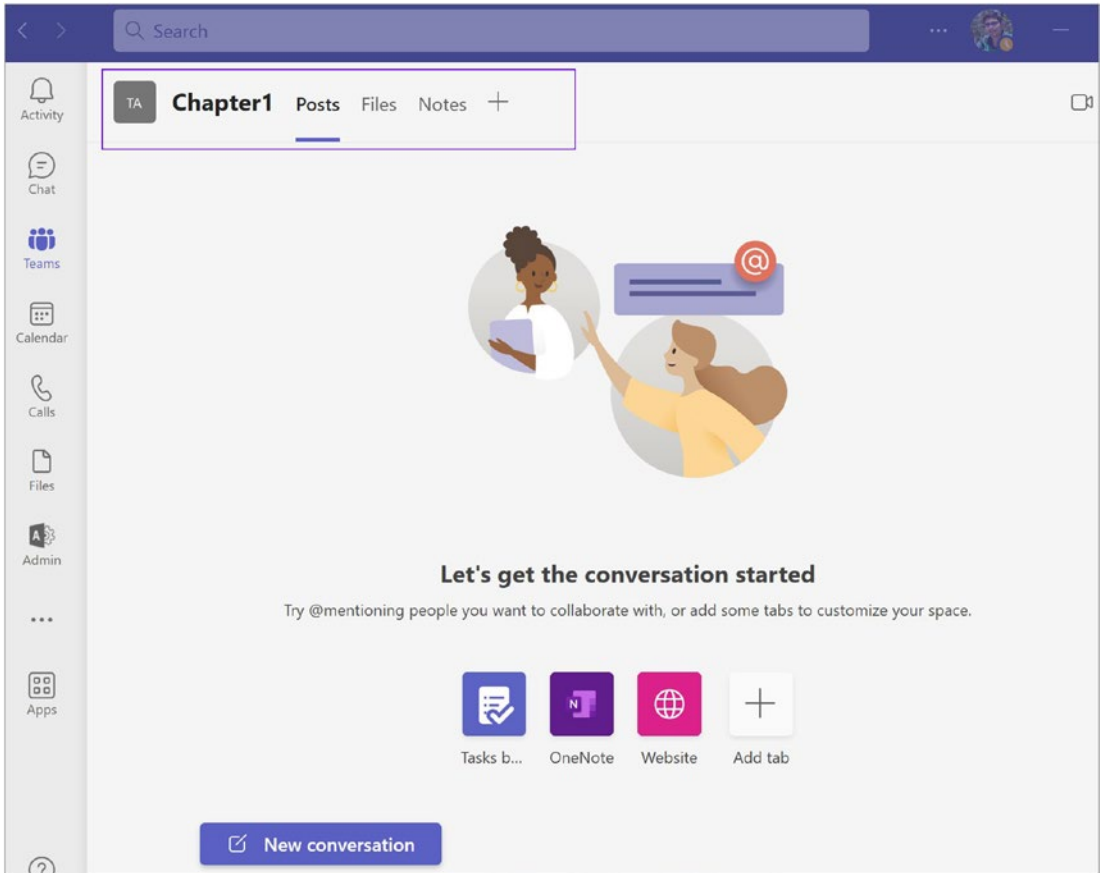


Figure 2-12. Channel created

When you click the “Add tab” plus sign (+), you will see multiple applications that can be added as tabs to your channel, as shown in Figure 2-13.

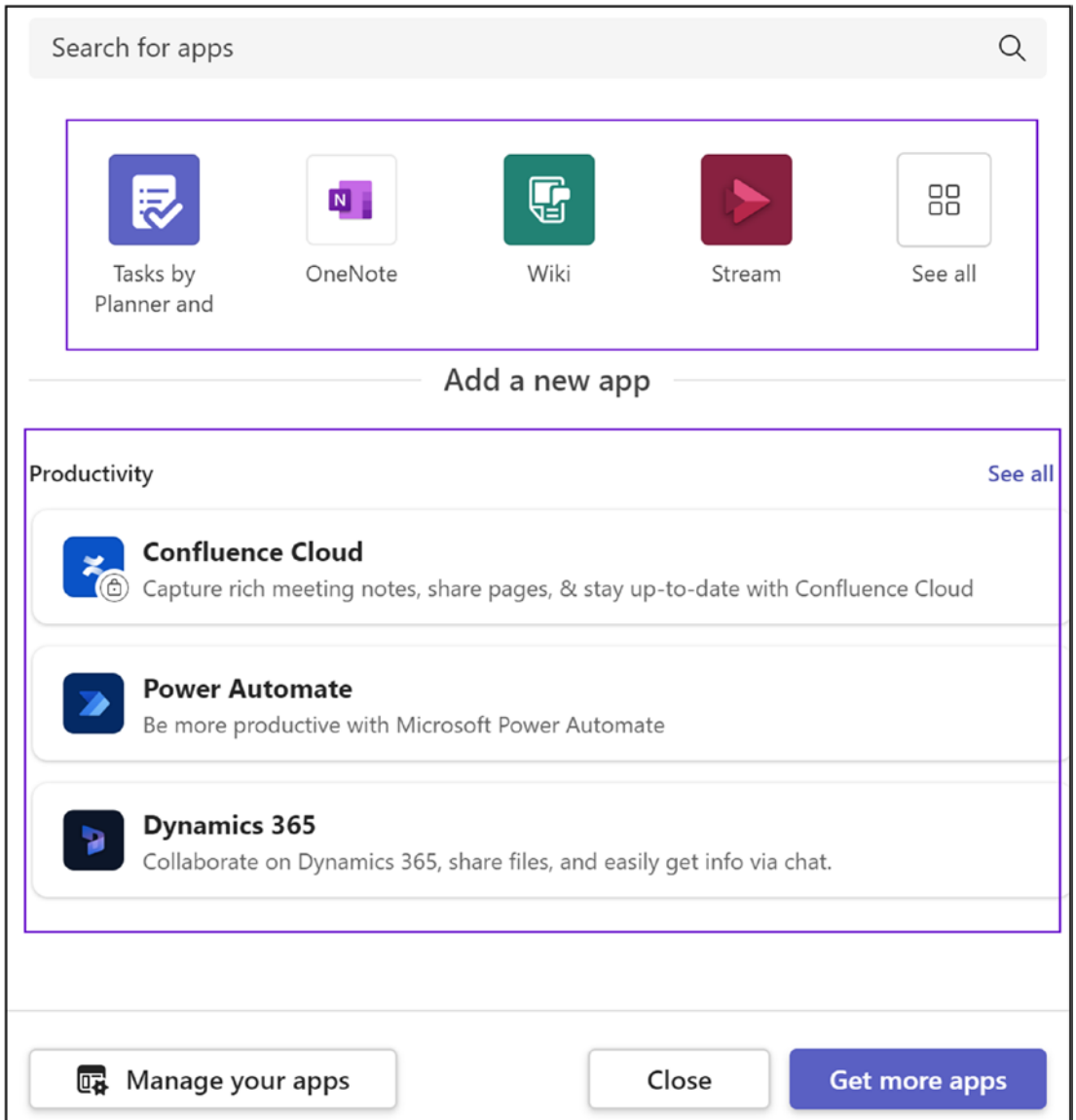


Figure 2-13. Applications to add as tabs

The other channel privacy mode is private. This type of channel focuses on private collaboration within a team. Private channels are different than standard channels, and they are already rolled out and available in Teams for use. It is important to notice from an architecture perspective that things are a bit different for private channels; for example, information that is shared in a private channel is stored differently than information stored in a standard channel because each private channel has its

own SharePoint site collection with file sharing enabled. Microsoft is making sure that information shared in a private channel is available only to the private channel members, not to all Teams members. Because each private channel has its own SharePoint site collection, Microsoft has increased the site collection count from 500,000 to 2 million. Individually, a team can hold a maximum of 30 private channels, and every private channel can hold a maximum of 250 members. The 30 private channel limit is in addition to the 200 standard channel limit per team. When the team owner creates a team from an existing team, any private channels in the existing team will not carry over to the new team.

How Private Channels Work

Microsoft took a while to make private channels available because it was complex to make sure a private channel is truly private.

Remember, a private channel has its own SharePoint site collection. That means if your Teams has more private channels, then the site collection count will grow as well. It is therefore important to inform your users to create private channels only if it is necessary.

Private channel chat is also different than chat in standard channels. Any chat that happens in a private channel will not be stored in the Exchange Online mailbox of the Office 365 group, but instead those chats will be stored in the individual mailbox of the members of that private channel.

Who Can Create Private Channels

By default, anybody in your organization can create a private channel. You as an admin can control private channel creation at the tenant level or at the team level.

For the tenant level, you as an admin can define a policy in the Teams admin center so that users in your organization can create private channels. As a team owner, you can also control private channel creation in your team by clicking More Options, selecting Manage Team, and then clicking Settings. Clear the check mark next to the “Allow members to create private channels” check box, as shown in Figure 2-14.

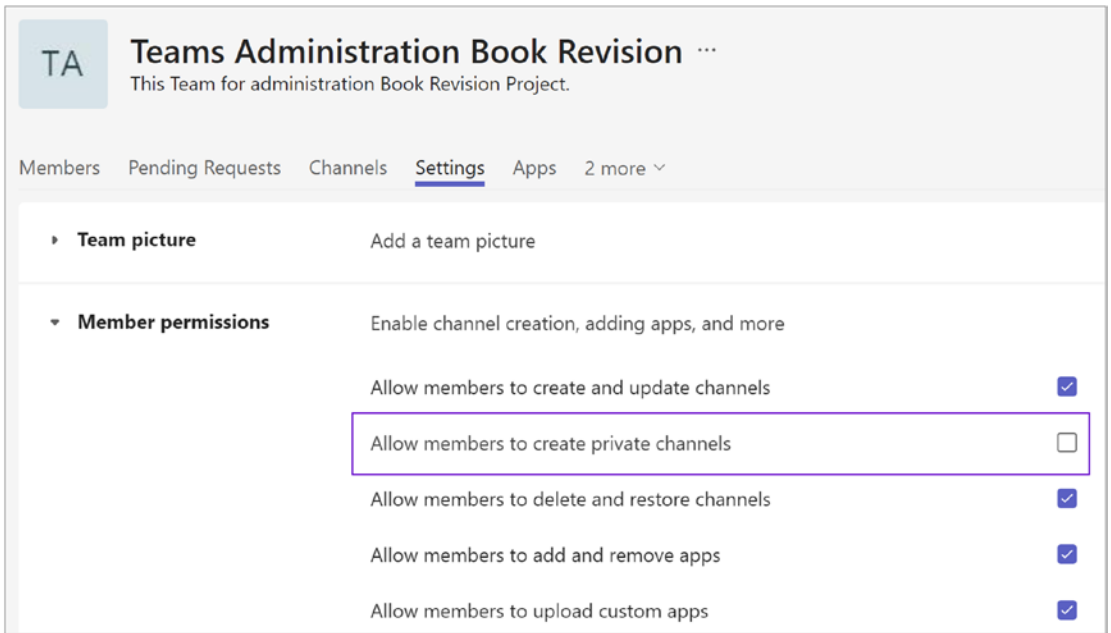


Figure 2-14. Private channel restriction setting (user level)

Creating a Private Channel

A private channel is accessible to specific people or a group that is added as a member of that private channel inside the team. To create a private channel, log in to the Teams app and expand the team under which you want to create the private channel. Click the more options icon (...) that is next to the team name, and you will see multiple options. Select Add Channel to create a channel, as shown in Figure 2-10. On the next screen, add a meaningful name and description to identify the private channel. Select “Private – Accessible only to a specific group of people within the team” to make the channel a private channel, as shown in Figure 2-15.

Create a channel for "Teams Administration Project" team

Channel name
Acknowledgement

Description (optional)
Help others find the right channel by providing a description

Privacy
Private - Accessible only to a specific group of people within the team

Cancel Next

Figure 2-15. Give a meaningful name and description to the private channel

After assigning a name and selecting the privacy type, on the next screen you need to add the members for the private channel. Because this is a private channel, only the people you add here will see this channel in Teams. If you want to add members later, just click Skip button, as shown in Figure 2-16.

Add members to the Acknowledgement channel

This is a private channel, so only the people you add here will see it.

Start typing a name Add

Skip

Figure 2-16. Adding members to a private channel

You will see the private channel has been created. Next to the channel name, you will see a lock icon that indicates that this is a private channel. Figure 2-17 shows that the Acknowledgement channel is a private channel.

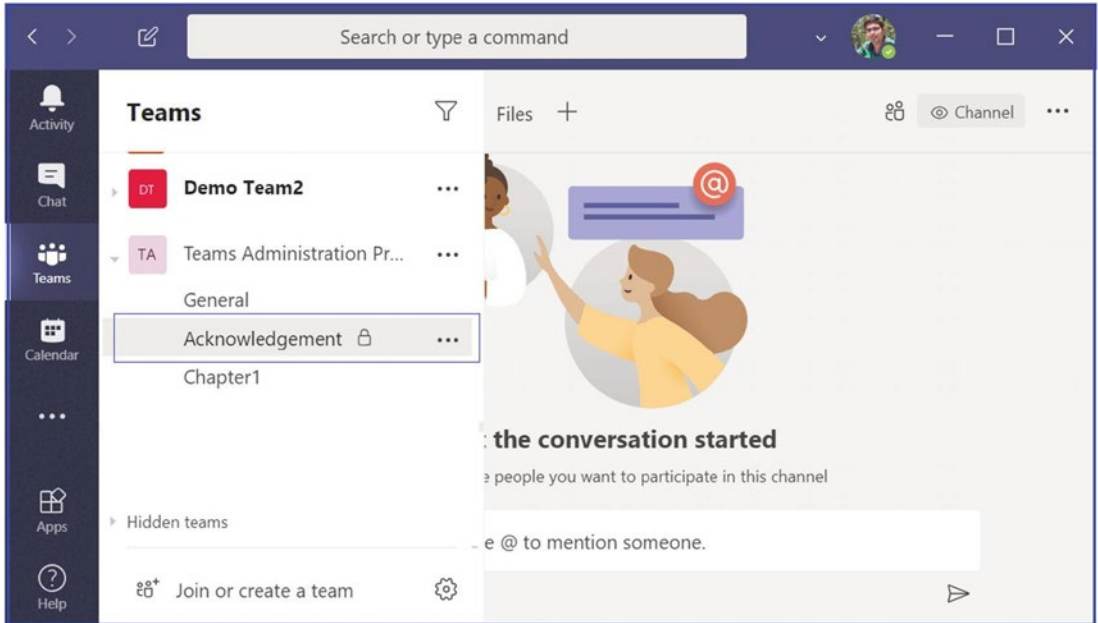


Figure 2-17. Private channel with a lock icon next to its name

Team Management Options

You as a team owner can manage your team settings. Figure 2-18 shows the team management settings that are available, including membership, guest access, and more.

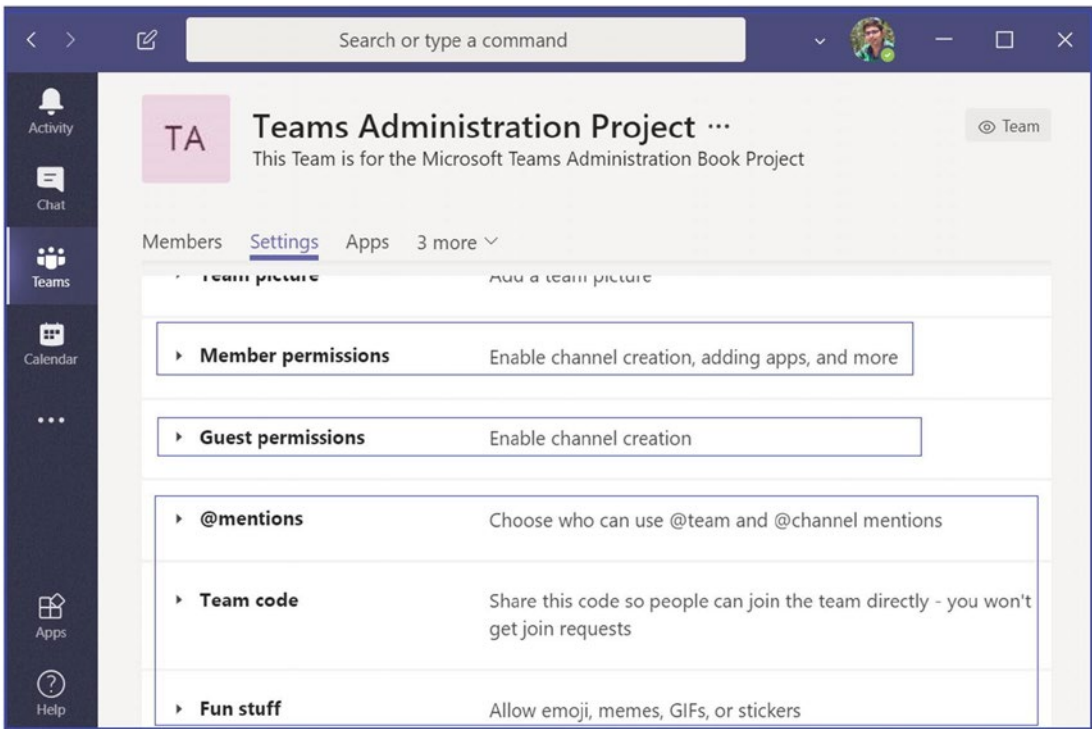


Figure 2-18. Team settings

Using the guest permissions settings, you can manage guest access for creating, updating, and deleting channels, as shown in Figure 2-19.

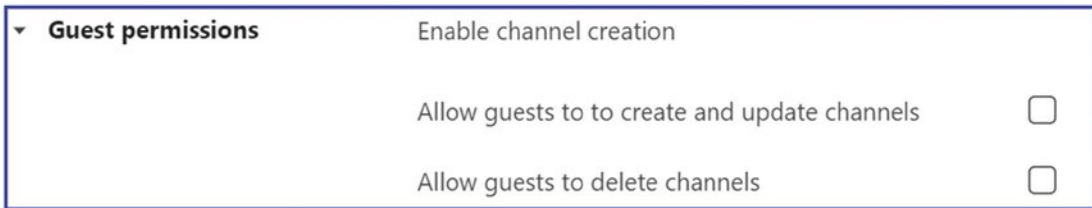


Figure 2-19. Guest permissions settings

The team owner can manage member permissions such as who can create or add apps, update channels, create private channels, and so on. Figure 2-20 shows all the available member permissions settings.

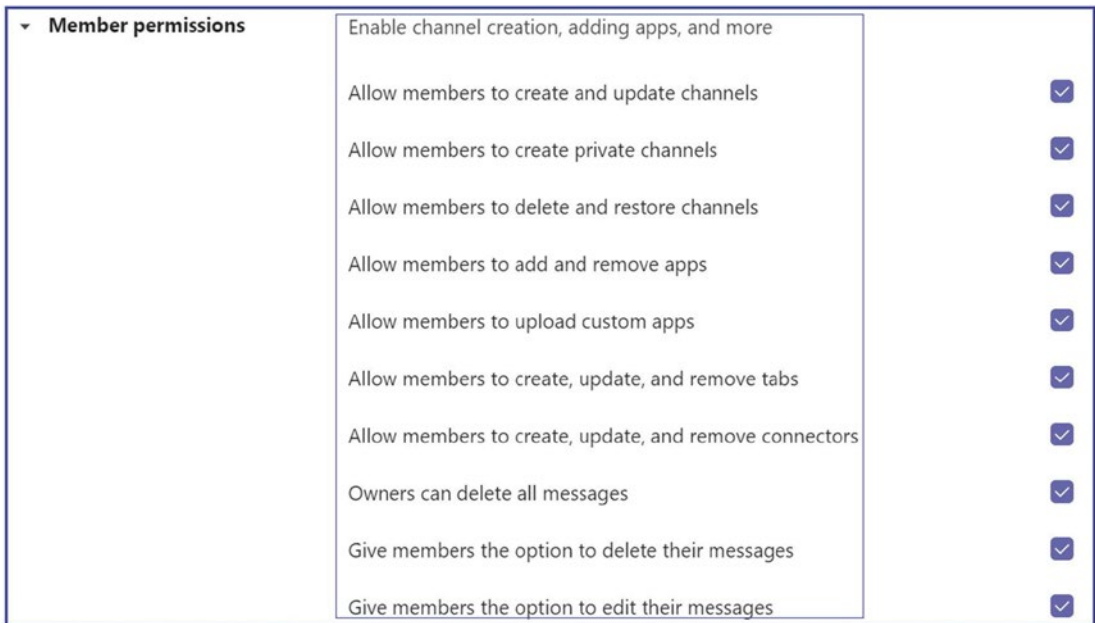


Figure 2-20. *Member permissions to control member access*

Every team has two roles: users and administrators. Users can be either owners, members, or guests of a team. The team owner is the person who creates the team. Team owners have authority to make any member of their team a co-owner when they invite them to the team or at any point after they have joined the team. It is best practice to have multiple team owners, which allows owners to share the responsibilities of managing team settings and membership, such as adding and removing members, adding guests, changing team settings, and handling administrative tasks. Team members are simply the individuals who the owners invite to join their team. Members can talk with other team members in conversations. They can view and usually upload and change files. They also can participate in the usual sorts of collaboration that team owners have permitted. Guests are individuals from outside of your organization, such as vendors, partners, or consultants, that a team owner invites to join the team. Guests have fewer capabilities than team members or team owners, but there is still a lot they can do.

Table 2-1 shows the different permissions that the team owner, members, and guests have to execute tasks. The listed permissions are based on the Teams desktop client; when using the Teams mobile client, you might see some differences.

Table 2-1. Team Owner, Member, and Guest Permissions to Execute Tasks

Ability to execute tasks	Owner	Member	Guest
Create a channel	✓	✓	✓
Participate in a private chat	✓	✓	✓
Participate in a channel conversation	✓	✓	✓
Share a channel file	✓	✓	✓
Share a chat file	✓	✓	✗
Add apps (such as tabs, bots, or connectors)	✓	✓	✗
Can be invited via any work or school account for Office 365	✗	✗	✓
Create a team	✓	✓	✗
Delete or edit posted messages	✓	✓	✓
Discover and join public teams	✓	✓	✗
View org chart	✓	✓	✗
Add or remove members and guests	✓	✗	✗
Edit or delete a team	✓	✗	✗
Set team permissions for channels, tabs, and connectors	✓	✗	✗
Change the team picture	✓	✗	✗
Add guests to a team	✓	✗	✗
Auto-show channels for the whole team	✓	✗	✗
Control @[team name] mentions	✓	✗	✗
Allow @channel or @[channel name] mentions	✓	✗	✗
Allow usage of emoji, GIFs, and memes	✓	✗	✗
Renew a team	✓	✗	✗
Archive or restore a team	✓	✗	✗

Note As you know, a team can be created from an existing Office 365 group. If this is the case, permissions are inherited from that group.

All users who have Exchange Online mailboxes can create a team.

Deploying and Managing Teams Clients

Microsoft Teams clients are available for all platforms, such as web clients, desktop (Windows, Mac, and Linux), and mobile (Android and iOS). So far, all clients require an active Internet connection and do not support an offline or cached mode, although this might change in the future. As a Teams admin, you will need to provide an installation method to distribute the Microsoft Teams client to computers and devices in your organization. For example, you can use System Center Configuration Manager (SCCM) for Windows operating systems or JAMF Pro for macOS.

Installing Teams Client on Desktop and Mobile

You can download the Teams desktop client (Windows or macOS) or mobile client by visiting <https://teams.microsoft.com/downloads>.

The Teams desktop client comes with a stand-alone (.exe) installer for user installation and works with MSI for Admin client rollouts. It is also available by default as part of Office 365 ProPlus. There is no special licensing for Teams clients. The desktop clients provide real-time communications support (audio, video, and content sharing) for team meetings, group calling, and private one-to-one calls. Also, Teams desktop clients can be downloaded and installed by an end user directly from the Microsoft Teams download site if the user has the appropriate local permissions.

Note Admin rights are not required to install the Teams client on a Windows machine, but they are required to install the Teams client on a macOS machine. Besides manual installation, admins can perform a bulk deployment of the Teams desktop client to selected users or computers in their organization. Microsoft

has provided MSI files (for both 32-bit and 64-bit) that let admins use Microsoft System Center Configuration Manager, Group Policy, or any third-party distribution mechanism for broad deployment. These files can be used to remotely deploy Teams so that users do not have to manually download the Teams app.

Distribution of the client through software deployment is only for the initial installation of Microsoft Team clients and not for future updates.

Getting the Teams Client Download for All Devices

Teams clients have a stand-alone application (.exe) installer for individual user installation available at <https://teams.microsoft.com/downloads>. When users visit the Teams download site, they will find all desktop (Windows 32- and 64-bit, macOS, and Linux DEB/RPM 64-bit) and mobile (iOS and Android) clients, as shown in Figure 2-21.

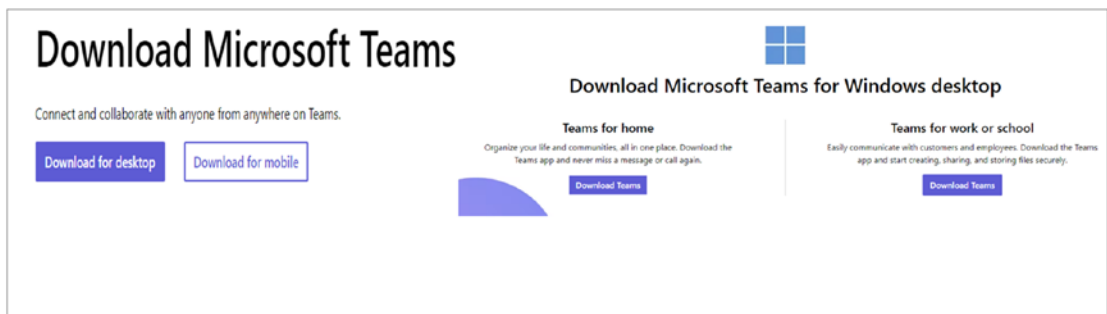


Figure 2-21. Getting the Teams client for all devices

The Microsoft Teams client is part of Office 365 ProPlus, which means when you install Office 365, the Teams client comes with it. The Teams client is part of update channels, including the Monthly channel and Semi-Annual channel. For more information, you can visit the Microsoft documentation for deploying Teams at <https://learn.microsoft.com/en-us/microsoftteams/get-clients>.

Teams Desktop Client Software and Hardware Requirements

For the best experience, a Windows desktop running Teams must meet the software and hardware requirements listed in Table 2-2.

Table 2-2. Teams Client Hardware and Software Requirements

Component	Requirement
Computer and processor	Minimum 1.1 GHz or faster, two core
Memory	4.0 GB RAM
Hard disk	3.0 GB of available disk space
Display	1024 x 768 screen resolution
Graphics hardware	Windows OS: Graphics hardware acceleration requires DirectX 9 or later, with WDDM 2.0 or higher for Windows 10 (or WDDM 1.3 or higher for Windows 10 Fall Creators Update)
Operating system	Windows 11, Windows 10 (excluding Windows 10 LTSC for Teams desktop app), Windows 10 on ARM, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2. Note: We recommend using the latest Windows version and security patches available.
.NET version	Requires .NET 4.5 CLR or later
Video	USB 2.0 video camera
Devices	Standard laptop camera, microphone, and speakers
Video calls and meetings	Requires two-core processor. For higher video/screen share resolution and frame rate, a four-core processor or better is recommended. Background video effects require Windows 10 or a processor with AVX2 instruction set. Joining a meeting using proximity detection in Microsoft Teams Rooms requires Bluetooth LE. Bluetooth LE on Windows requires Bluetooth to be enabled on the client device and requires the 64-bit version of the Teams client. This feature is not available on 32-bit Teams clients.

You might be wondering if you need to allow admin permission for a user to install the Teams client. The answer is no; you don't need admin permission to install the Teams client.

Teams Desktop Client for Windows

When a Microsoft Teams call is initialized by a user for the first time, the user might notice a warning with the Windows firewall settings that prompts users to allow communication. However, the user might be instructed to ignore this message because despite the warning, when it is dismissed, the call will still work. On Windows, the Teams desktop client requires .NET Framework 4.5 or later. If this is not installed on the computer, the Teams installer will offer to install it automatically.

Where Can I Find the Teams Client Installation?

The Teams client can be installed on a per-user basis. This means if a computer is shared and more than one user accesses the same computer, every individual accessing the computer can install the Teams client on their own login profile. The Teams client is installed to the directories listed here and updated in separate directories. Figure 2-22 shows the Teams directory.

- Teams application
 - %LocalAppData%\Microsoft\Teams
 - %LocalAppData%\Microsoft\TeamsMeetingAddin
 - %AppData%\Microsoft\Teams
- Update directories
 - %LocalAppData%\SquirrelTemp

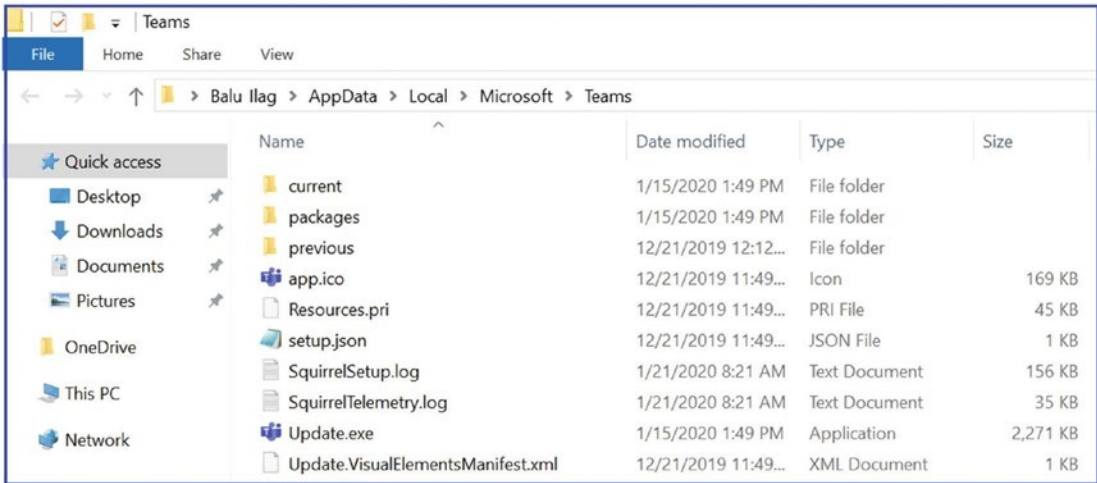


Figure 2-22. Teams installation directory

Note For Teams admin control of installation, all of the directories just mentioned can be accessed and controlled.

Microsoft Teams Desktop Client MSI Deployment

The Microsoft Teams desktop client can be deployed to computers in your organization by using the Microsoft Teams MSI package. The Teams MSI package will place an installer in Program Files, which will in turn install the Teams Machine-Wide Installer on each user profile logged into a machine.

Microsoft allows for Teams (MSI) client rollout through existing standard deployment processes such as Group Policy, SCCM, Intune, or third-party tools. You as an admin must determine which computers already have the Teams client installed and which are newly built with an operating system. Usually, you can add the Teams client in the operating system build so that all newly built computers will have the Teams client installed.

Deploying the Teams MSI Client

As an admin, you can use MSI deployment for the Teams client; however, you cannot deploy the client updates. When the Teams client is deployed, the Teams MSI installer is located in the Program Files directory. Whenever a new user signs in, Teams will be installed and then started automatically. After the Teams client starts, the user is signed in, and the update process begins. If the Teams version is new enough, the user will be able to use the Teams client (the update happens in the background). If the Teams version is old, the Teams client will update itself, but the user will have to wait for the update to be completed.

The Teams MSI installer also allows you to disable client autostart. Once the Teams client rollout is complete, all users will have the Teams client on their computer, and it automatically starts when they log in to their computer. However, if end users don't want Teams client to start automatically, the MSI installer allows you to disable the initial automatic launch of Teams. Also, the Teams client shortcut will be placed on the user's desktop.

Note Once the user manually starts the Teams client, it will automatically start at startup.

To disable the Teams client autostart for the 32-bit version, run this command at the command prompt: `msiexec /i Teams_windows.msi OPTIONS="noAutoStart=true"`. For the 64-bit version, run this command at the command prompt: `msiexec /i Teams_windows_x64.msi OPTIONS="noAutoStart=true"`.

Note If you run the MSI manually, be sure to run it with elevated permissions. Even if you run it as an administrator, without running it with elevated permissions, the installer will not be able to configure the option to disable autostart.

Managing the Teams Desktop Client

Microsoft has made Teams client management simple.

Uninstalling Teams Completely from a Computer

If the Teams client is installed but not working correctly or you want to uninstall the Teams client for any other reason, make sure to uninstall the client completely; otherwise, the MSI installer won't install the Teams client again. To completely uninstall the Teams client on your computer, first uninstall the Teams client from every user profile that was installed earlier using Start ► Control Panel ► Program Files. Locate Microsoft Teams, and then click Uninstall. After uninstallation, delete the Teams directory recursively under `%LocalAppData%\Microsoft\Teams`.

Microsoft has provided a cleanup script for the uninstallation steps for SCCM, which you can get from <https://aka.ms/AA2jib>.

Updating the Teams Client

Microsoft designed the Teams client to be updated automatically so that users will always have an updated client with the latest bug fixes, feature improvements, and new capabilities. Hence, you as an admin cannot control or manage Teams client updates.

The Teams client update process includes multiple checks. For example, when a user signs into Teams, validation occurs. If the Teams client version is not up-to-date (more than three versions old), then Teams updates are made before the client can sign in.

If the Teams client is not outdated, the user can sign in and use the client, but the Teams client will check for new updates after 15 minutes in the background. If an updated version is available, Teams will download the updated Teams full client package. It will be installed when the Teams client is idle for 30 minutes. After the Teams client installs the updated version, it will restart and send a notification to the user indicating that the Teams client has been updated.

As per Microsoft, Teams client updates are expected every two weeks, excluding hotfixes, which are deployed whenever required.

Note If the Teams client is older than three versions, the Teams client cannot sign in before the client updates.

Managing Teams Client Configuration

Currently, the Microsoft Teams client behavior is controlled via policies that are defined and managed in the Teams admin portal and PowerShell. As of now, there are no options to manage the Teams client via Group Policy or the registry keys. For example, the features that Teams client displays, including voice and video calls, are controlled via the Teams admin center policies for all the clients. As another example, Outlook add-ins can be enabled or disabled through the Teams admin center meeting policies. However, there is nothing that can be managed or controlled via Group Policy or a registry key. Microsoft might or might not change this behavior in the future.

When the Microsoft Teams Outlook Add-in Is Not Installed

When a Microsoft Teams desktop client installs on a computer, the Teams meeting add-ins in Outlook are added automatically, allowing users to schedule Teams meetings. However, if somehow the Teams meeting add-ins are not visible, the user cannot schedule Teams meetings using Outlook. This happens because Teams might fail to initialize the add-in. To resolve this, follow these steps. Note that these steps are required only the first time to initialize the add-ins.

1. Make sure Outlook is open before the Teams client is started. You can simply close both the Teams client and the Outlook client (you can use Task Manager to completely close teams.exe and outlook.exe; see Figure 2-23).

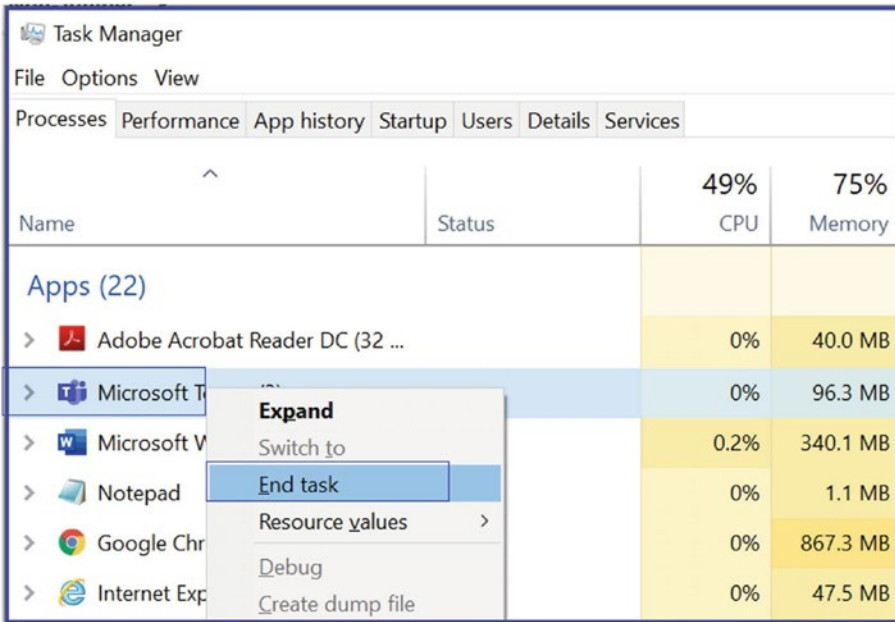


Figure 2-23. Closing the Teams client completely

2. Open or start Outlook first and then start the Teams client.

Most important, the Teams outlook add-in will be disabled depending on the Teams upgrade coexistence mode selected for the tenant or the specific user in the Teams admin center. For example, if a user’s Teams upgrade mode selected Skype for Business Only, then the Teams meeting add-in will not show in Outlook. Also, as mentioned earlier, the meeting add-in can be disabled via Meeting Policy in the Teams admin center.

For Mac operating systems, users can install the Teams client by using a PKG installation file for macOS computers. Administrative access is required to install the Mac client. The macOS client is installed in the /Applications folder. To install Teams using the PKG file, perform the following steps:

1. Visit the Teams download page at <https://teams.microsoft.com/downloads#allDevicesSection>. Under Desktop, click Mac to download the file.
2. Double-click the PKG file.
3. Follow the installation wizard to complete the installation.
4. Teams will be installed to the /Applications folder; it is a machine-wide installation.

On Linux operating systems, the Teams client for Linux is available for users as native Linux packages in .deb and .rpm formats. To download the Linux DEB (64-bit) or RPM (64-bit) client, visit <https://teams.microsoft.com/downloads#allDevicesSection>, click Linux DEB or RPM, and then install it.

Virtual Desktop Infrastructure (VDI) is virtualization technology that hosts a desktop operating system and applications on a centralized server in a data center. With VDI, users can enjoy a fully personalized desktop experience with a fully secured and compliant centralized source.

Deploying the Teams Mobile Client

As previously mentioned, Microsoft Teams mobile apps are available for Android and iOS. Users can download the mobile apps through the Apple App Store and the Google Play Store. Currently there are two supported mobile platforms for Microsoft Teams mobile apps: Android (5.0 or later) and iOS (10.0 or later). Once the mobile app has been installed on a supported mobile platform, the Teams mobile app itself will be supported provided the version is within three months of the current release.

Note Teams mobile app distribution is not currently supported using a mobile device management (MDM) solution. Microsoft might support Teams mobile app distribution through MDM in the future.

Monitoring Teams Client Usage

As a Teams admin, when you roll out the Teams desktop and mobile clients in your organization, the next important step is to monitor the Teams client usage per the operating system or device. You can monitor the Teams client device usage using the Teams admin portal.

To get a Teams client device usage report, log in to the Office 365 admin center portal by visiting <https://admin.microsoft.com/Adminportal/Home>. Click Report and then select Usage. On the Usage page, select Microsoft Teams and choose Device Usage. Figure 2-24 shows an example Teams client device report. On the report page, you can choose Users or Distribution; Figure 2-24 shows the Teams device distribution report.

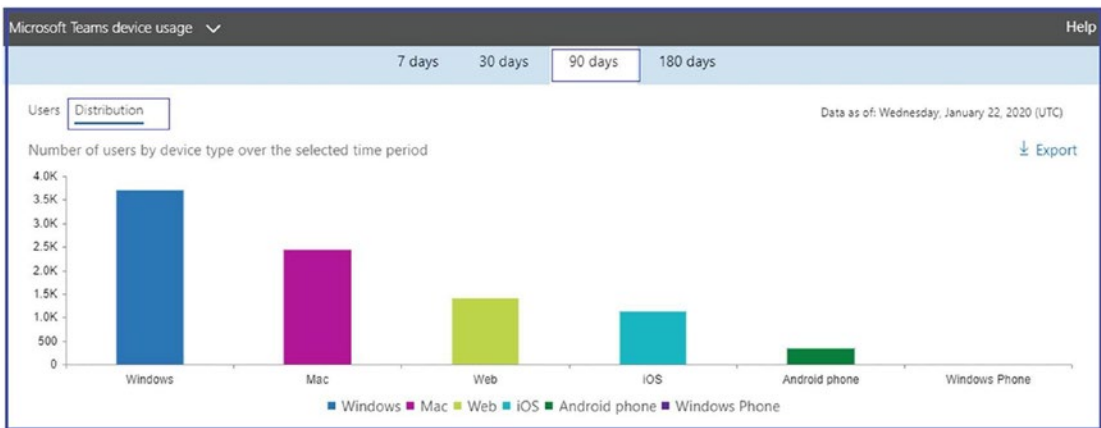


Figure 2-24. Teams client device usage report

The Teams device report is available for different durations, including 7 days, 30 days, 90 days, and 180 days. The report will allow you to receive per-user basis usage as well.

Configuring and Managing Live Events and Microsoft Stream

Microsoft Teams provides different formats for interactive and large broadcast events such as Teams meetings and live events within your organization, with both internal and external meeting participants. As an admin, you must understand the configuration, settings, and policies that can be used in Teams Live events and Microsoft Stream.

Chapter 1 covered topics like what live events and Microsoft Stream are, their architecture, live event scheduling, how Stream stores users' meeting recordings, how users can access the recordings, and so on. If you are still new to live events and Microsoft Stream, review Chapter 1 before continuing.

In this section, you are going to learn the step-by-step process for configuring policies and settings so that you as an admin can provide your users with the optimal user experience during live events and when using Microsoft Stream for meeting video recording and sharing content.

After learning about these topics, you will be able to do the following:

- Configure live event settings
- Manage and create live event policies
- Manage Microsoft Stream

Overview of Live Events

Microsoft Teams Live events are a scalable and ideal solution for online meetings for an audience up to 20,000 with four-hour duration. Microsoft Teams Live events are ideal for webinars, presentations, conferences, or company-wide announcements. Live events are highly customizable and offer various roles such as organizer, producer, presenter, and attendee each with specific capabilities and permissions. Live events scale online meetings to audiences with thousands of concurrent viewers. In the background, Teams leverages artificial intelligence for meeting assistance for features such as captions and translation. Captions are useful when attendees have audio limitations or need language translation. Optionally you can enable Q&A Manager and Yammer social feed integration to interact with audience members. You can record the event with video and after the live event provide an attendee engagement report for consumption insights, such as how many people joined and how long they stayed with an event.

Live events work very well because they enable high-quality, adaptive video streaming that can be consumed on any Teams-enabled devices, including Windows, macOS, and mobile devices, and devices that don't have the Teams client installed through a browser. Live events are delivered with minimal lag from worldwide Microsoft data centers, so no matter where your tenant is located and users are located, live events always find a shorter path for users to connect to the event to avoid latency. Also, large organizations can use a third-party eCDN partner to save corporate bandwidth.

With limited knowledge, anyone can use live events, and they can be scheduled easily in Teams. Users can present and produce live events from the macOS or Windows Teams client with one or more presenters, including application sharing. You can present from the Teams room system, or presenters can dial in from a phone line to a live event using Teams audio conferencing. As a live event organizer, you can control access to the event for everyone from an organization to specific groups or people.

Before configuring live event policies and settings, an admin must know who can use and schedule live events based on license requirements and permissions. To use live events, users must have a user account in Azure AD; the user cannot be a guest or from another organization. Apart from the Azure AD account, users must have a Microsoft 365 Enterprise E1, E3, or E5 license or a Microsoft 365 A3 or A5 license. Users must also have permission to create live events in the Microsoft Teams admin center and in Microsoft Stream for events produced using an external broadcasting app or device. Finally, users must have private meeting scheduling, screen sharing, and IP video sharing turned on in a Teams meeting policy with an Exchange Online mailbox.

Configuring and Managing Live Events Settings

Teams Live events settings allow you to control organization-wide settings for all live events that are scheduled. An admin can decide to include a support URL when live events are held and set up a third-party video distribution provider for all live events organized and scheduled by people in an organization.

Settings for the live events that are organized within your organization can be configured in the Microsoft Teams admin center. Remember, live event settings will be applied to all live events that are going to be created in the organization.

Microsoft has provided two different ways to configure Live event settings: using the Teams admin center and using PowerShell.

Configuring Live Event Settings Using the Teams Admin Center

To configure live event settings using the Teams admin center, follow these steps:

1. Log in to the Microsoft Teams admin center with your admin credential (you must have Teams service admin or global admin permission configure live event settings).

- After you log in to the Teams admin center, navigate to Meetings and then select Live Events Settings (see Figure 2-25). If you have an internal support URL, replace the default URL with the support URL that will be shown to the attendees who will participate in the live event. You can also enable third-party video distribution providers.

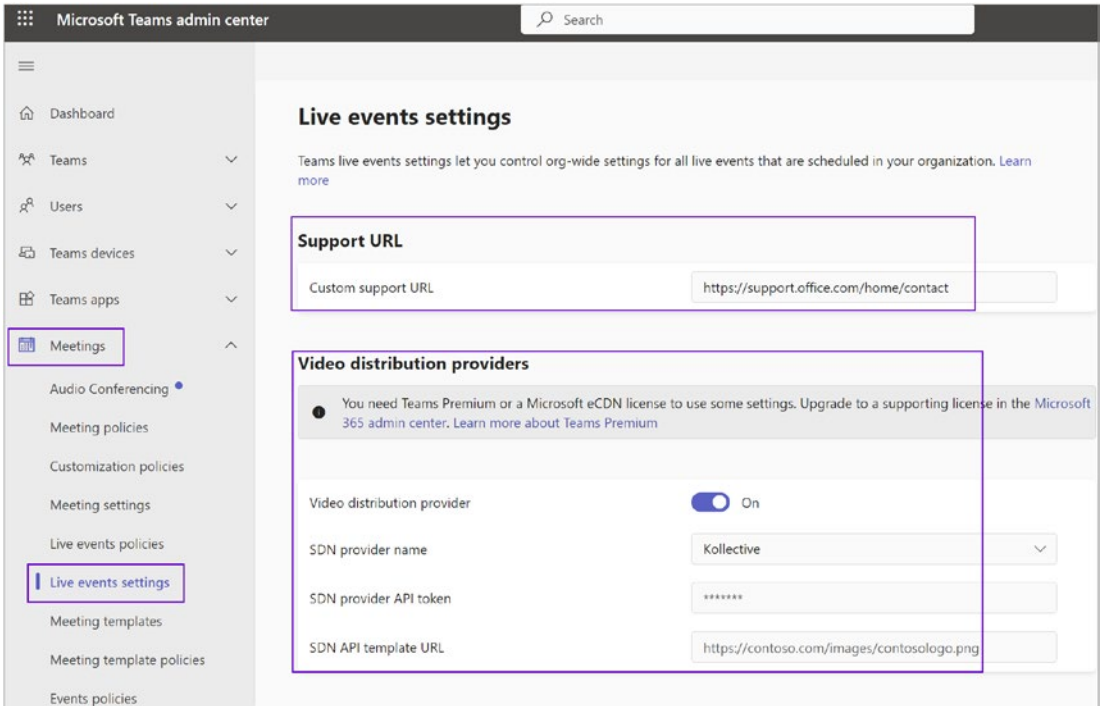


Figure 2-25. Live event settings

If you have a third-party distribution provider, select the appropriate one. The example shown in Figure 2-26 has Collective selected as the provider. Enter the software-defined networking (SDN) provider API token you received from your provider and then enter the SDN template URL you received from your provider. There currently are five distribution providers: Microsoft eCDN, Hive, Collective, Riverbed, and Ramp.

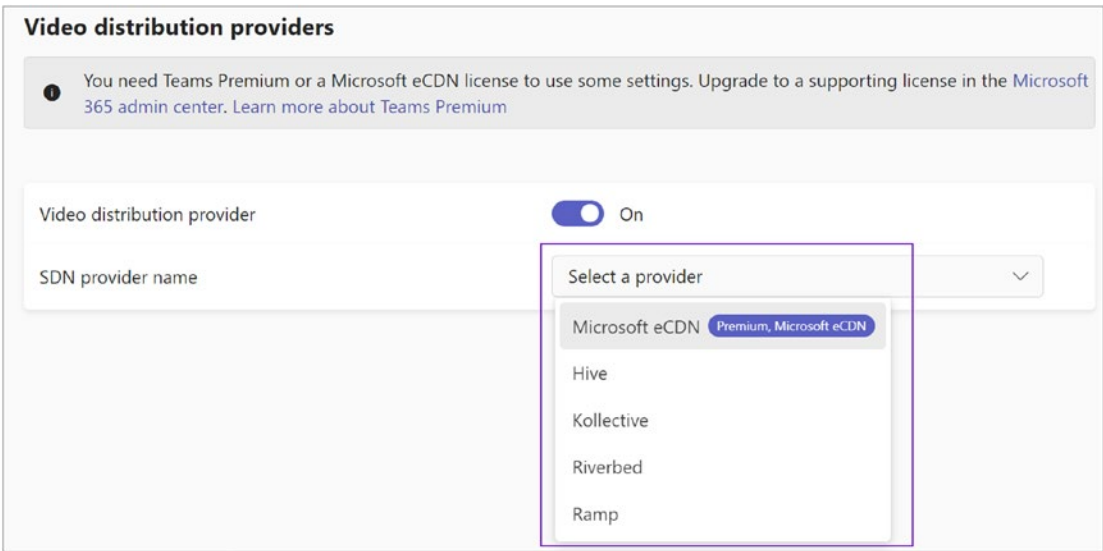


Figure 2-26. *Third-party distribution providers*

3. Finally, click Save button to commit the configuration changes.

Configuring Live Event Settings Using PowerShell

Perform the following steps to configure the live event settings for the support URL and a third-party distribution provider using Windows PowerShell. To set up the support URL using PowerShell, you should connect to the Microsoft Teams Online PowerShell module and then run the following command:

```
Set-CsTeamsMeetingBroadcastConfiguration -SupportURL "Org Support URL"
```

Here's an example:

```
Set-CsTeamsMeetingBroadcastConfiguration -SupportURL "https://bloguc.com/Support"
```

Next, if you want to configure your third-party video provider using Windows PowerShell, you must first acquire a provider API token and API template from your provider contact. Once you have that information, you should run the following command (in this example, the provider is Collective Streaming):

```
Set-CsTeamsMeetingBroadcastConfiguration -AllowSdnProviderForBroadcast  
Meeting $True -SdnProviderName Collective -SdnLicenseId {license ID GUID  
provided by Hive} -SdnApiTemplateUrl "{API template URL provided by Hive}"
```

Note If you want to create live events using an external encoder or device, you must first configure your eCDN third-party provider with the Microsoft Stream admin center as well.

Configuring and Managing Live Events Policies

As an admin, you can modify existing live event policies or create new policies. A live event policy allows admins to control which users in the organization can host live events, as well as which features are going to be available in the events they create. By default, a Global (Org-wide default) live events policy is available. Admins can modify this policy or create one or more custom live event policies. After a custom policy is created, it should be assigned to a user or groups of users within the organization.

Note The live event Global (Org-wide default) policy is already assigned to every individual in your organization. If you have not created and assigned any custom policy, all users will receive the default policy.

Figure 2-27 shows the default policy with these settings: live event scheduling is enabled for Teams users, live captions and subtitles are turned off, everyone in the organization can join live events, and the recording setting is set to always record.

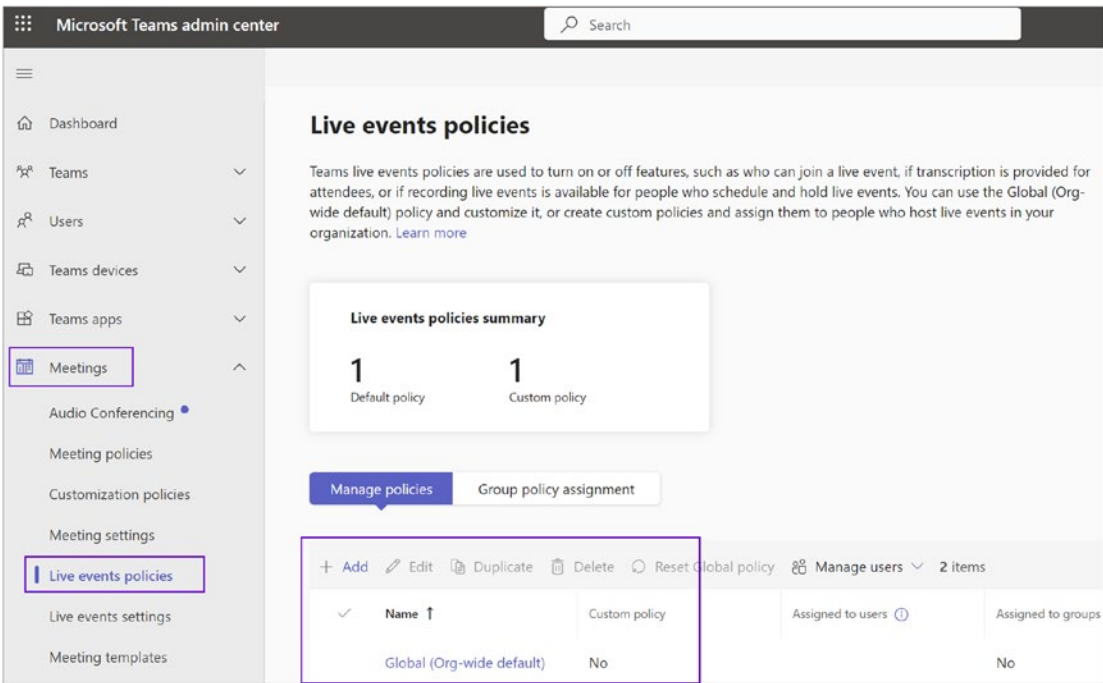


Figure 2-27. Default Global (Org-wide) policy in live event

Microsoft has provided two different ways to configure live event policies: using the Teams admin center and using PowerShell.

Creating a New Live Event Policy Using the Teams Admin Center

Log in to the Teams admin center, navigate to the Meetings tab, and then select Live Event Policies. You can choose to create or manage/edit live event policies. When doing so, you can manage the following options:

- *Global policy:* This organization-wide policy is the existing default policy. You can click Edit to make changes to this policy.
- *New policy:* This option is used to create a new custom policy.
- *Choose existing policy:* By selecting this option, along with an existing policy and the Edit button, you can make changes to that policy.

Creating a New Policy

Follow this procedure to create a new live event policy. Log in to the Teams admin center, navigate to Meetings, and click Live Event Policies. Click the +Add button, and then enter the required inputs, as shown in Figure 2-28.

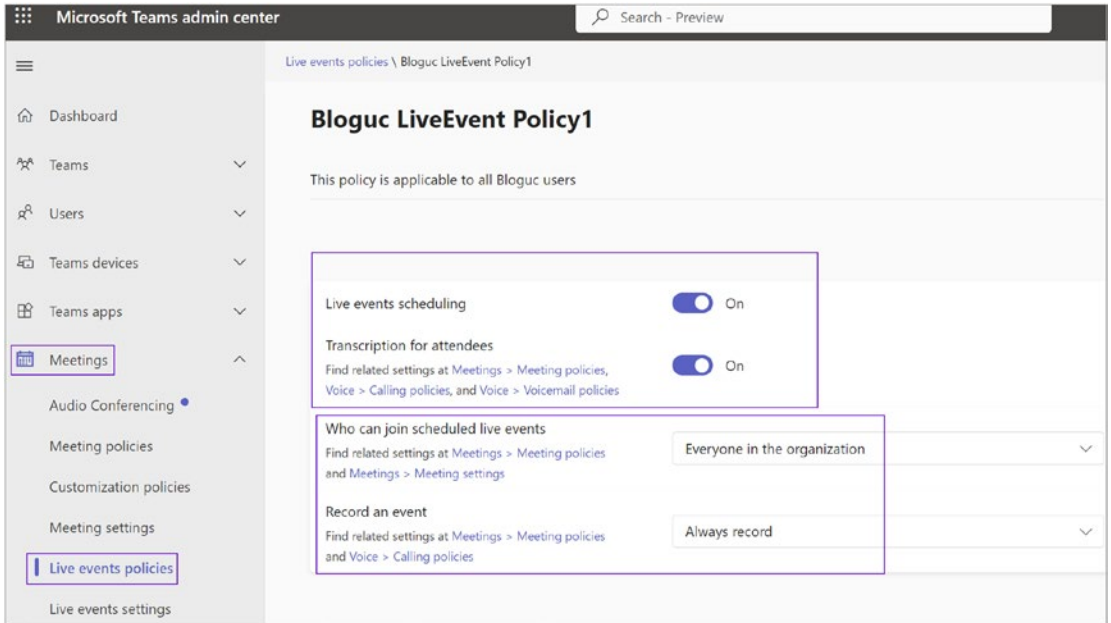


Figure 2-28. *Creating a new live event policy*

On the new event page, type a meaningful name for your policy, and optionally type a description. This example uses the name Cyclotron LiveEvent Policy1 and includes a description. Next, customize the following settings according to your preferences for this new policy:

- *Allow scheduling:* You must allow this so that the users will be able to schedule live events.
- *Allow transcription for attendees:* This allows transcription.
- *Who can join scheduled live events:* Select from Everyone, Everyone in the organization, and Specific users or groups. In this example, Everyone In The Organization is selected.

- *Who can record an event:* Select from Always record, Never record, and Organizer can record. Figure 2-29 shows “Always record” as the selected setting.

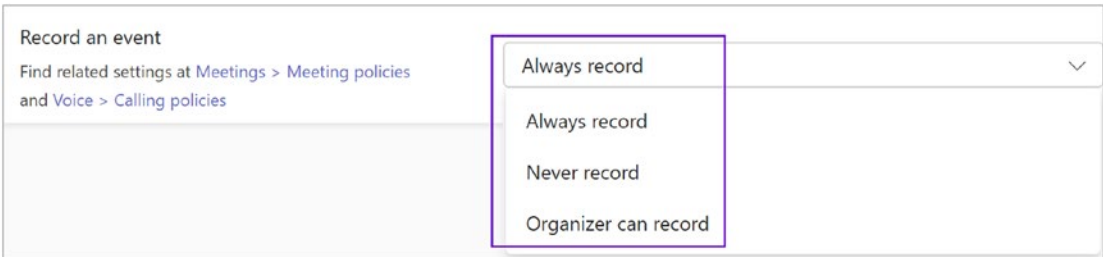


Figure 2-29. *Who can record a live event*

Finally, click Save to commit the new policy changes.

Managing Microsoft Stream

An overview of Microsoft Stream and its architecture was covered in Chapter 1. Here we specifically cover Microsoft Stream management.

To review, Microsoft Stream is a Microsoft enterprise video solution that is part of Office 365. Customers can use Microsoft Stream to securely carry and deliver videos to their organization. Stream supports live events through Teams, Stream, and Yammer. Microsoft provides a portal to upload, share, and discover videos such as executive communication or training and support videos. Microsoft Stream allows users to upload videos, search groups and videos, broadcast their live events, and provide a way to categorize and organize videos. Users can also create a group, and Stream allows users to embed video in Microsoft Teams.

Stream supports Teams video recording, as when a user records a Teams meeting by clicking the record button in a Teams meeting. That recording goes over Stream, and all of the sources are fully integrated with Stream, including automatic transcripts, a search function, and the enterprise security that customers expect from Microsoft Office 365 services.

There are two ways to access Microsoft Stream.

- You can access Microsoft Stream by visiting <https://web.microsoftstream.com>.

- You can access Stream using the Office portal. Log in to office.com. Click the Office 365 app launcher icon, select All Apps, and then select Stream. Alternatively, go to stream.microsoft.com and sign in with your work or school credentials.

When you log in to Microsoft Stream, you can see the Discover, My Content, and Create options. Under Discover, the Videos, Channels, People, and Groups settings are available for your organization, as shown in Figure 2-30.

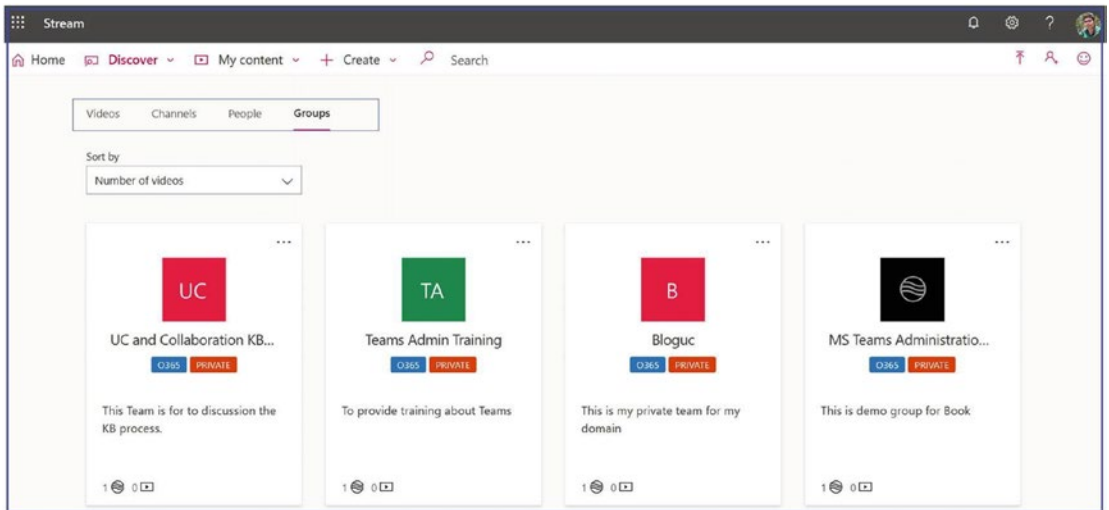


Figure 2-30. Microsoft Stream Groups view

Organizing and Managing Groups and Channels in Stream

When you create a group in Stream, it actually creates a group in Office 365, which means groups in Stream are built on top of Office 365 Groups. When you make a group in Stream, it creates a new Office 365 group that can be used across Office 365, giving the group an email address, calendar, group site, and so on. If you already use Office 365 Groups in your organization from Microsoft Teams, SharePoint, Viva (Yammer), Planner, and so on, you can start using those groups in Stream right away.

In Microsoft Stream, you can use channels and groups to organize and grant permission to your videos. Specifically, groups in Stream are used to control video access and organize videos. Each group has both owners and members. Each group gets its own

video portal, with a highlights page showing trending and new content within the group. A group's videos can be further organized by creating channels within the group. It is best practice to put a video into one or several groups to help viewers find it more easily.

Important Remember, deleting a group in Stream will also permanently delete the Office 365 Group and everything associated with the group. This includes videos, conversations, files, and content for all the Office 365 group-enabled services such as Outlook, SharePoint, Teams, Planner, Yammer, and so on.

Channels provide an organization technique for videos, but not a permission approach. Channels don't have any permissions on their own. If viewers follow your channel, they can get updates when new videos are added. You can put a video into one or several channels to help viewers find it more easily.

When you create a channel, you decide whether it's an organization-wide channel that anyone in your organization can add and remove videos from or if it's a group channel where you can limit contributors. If you are interested in learning more, visit the Microsoft documentation at <https://docs.microsoft.com/en-us/stream/groups-channels-overview>.

Administrative Tools

The following sections cover the administrative tools.

Managing Teams Using the Microsoft Teams Admin Center

The Microsoft Teams admin center is one place where most of the Teams service-side configuration and management resides. Using the Teams admin center, admins can manage the Teams services the way an organization wants to manage the Teams experience for its users. This is similar to other Office 365 applications. There are multiple admin tools available; however, from a graphical user interface (GUI) perspective, there are three main admin tools, including the Microsoft Teams admin center. This is where you manage all Teams-related settings and policies for

communications and Teams-specific features such as Teams meetings, messaging and calling policies, Teams organization-wide settings, guest and external access, application permissions, and so on.

This section will provide extensive details about Microsoft Teams administration including all that the Teams admin center provides.

Accessing the Teams Admin Center

Admins can access the Teams admin center through the Office 365 portal or by directly visiting the Teams admin center at <https://admin.teams.microsoft.com/>.

In addition to the previously mentioned GUI tools, you can use PowerShell to manage the Teams experience. Microsoft provides a Teams module as well, and to some extent you can use the Microsoft Teams graph API. It's entirely up to you to use whichever solution is suitable for the Teams management perspective in your organization.

Understanding the Teams Admin Role

Many organizations that use Teams have more than one admin managing the Teams workload and supporting the Teams functionality. In many cases, you don't want to have same the access permissions for every admin, and that's where the Teams admin role comes in.

A Teams admin has four different roles that you can designate to Teams administrators who need different levels of access for managing Microsoft Teams. That gives every Teams admin the correct required permissions. The following are the roles that are available to manage Teams:

- *Teams Administrator (Service)*: This admin role can manage the Teams service and manage and create Office 365 groups.
- *Teams Communications Administrator*: This admin role can manage calling and meeting features within the Teams service.
- *Teams Communications Support Engineer*: This admin role can troubleshoot communication issues within Teams using advanced tools.

- *Teams Communications Support Specialist*: This admin role can troubleshoot communications issues within Teams using basic tools.
- *Teams Device Administrator*: This role can manage device configuration and updates, review device health and status of connected peripherals, set up and apply configuration profiles, and restart devices.

If you are interested in learning more about each role and its capabilities, visit <https://docs.microsoft.com/en-us/microsoftteams/using-admin-roles>.

Teams Administration Through the Teams Admin Center

The Microsoft Teams admin center is an online portal designed specifically for IT administrators to manage the Teams platform across their organization. It provides admins with a central place to handle settings, users, teams, and policies, enabling efficient and effective management of the Teams environment.

Key Uses of the Microsoft Teams Admin Center

Here are some of the core functions and tasks you can accomplish using the Microsoft Teams admin center:

- *Manage teams*: Admins can view and manage all teams in the organization, including creating new teams, changing team settings, managing membership, and deleting teams. They can also manage team templates to streamline the process of creating new teams.
- *Manage users*: This includes adding and removing users, assigning roles and permissions, and managing user settings.
- *Manage policies*: Admins can create and manage various policies that govern the features and capabilities available to users, such as meeting policies, messaging policies, app setup policies, and live events policies.
- *Manage meeting settings*: These include global settings for meetings like default meeting settings, meeting expiration times, and cloud recording options.

- *Analytics and reporting:* The admin center provides extensive analytics and reporting options, helping admins monitor usage, performance, and user activity. This includes call quality, user activity reports, and device usage reports.
- *Manage voice and calling features:* Admins can manage Teams calling features such as call queues, auto attendants, call park policies, and more.
- *Manage apps:* Admins can manage the apps available to users, set up app permission policies, and control app setup policies.
- *Manage devices:* Admins can manage certified Teams devices, monitor device health, and update device settings from the admin center.

To log in to Microsoft Teams admin center, you must have one of the role permissions just covered or the Office 365 Global admin permission. When you log in to the Teams admin center, you will see different views based on your access permissions. For example, if you have Teams Communication Support Engineer or Teams Communications Support Specialist role permissions, you will see only the Users and Call Quality Dashboard options on the Teams admin center dashboard.

I have logged in to the Teams admin center (<https://admin.teams.microsoft.com/>) using my Teams Admin (Service) role permission to see all admin tools and options to manage Teams for my demo tenant. Figure 2-31 shows the ideal Teams admin dashboard that a Teams admin can see.

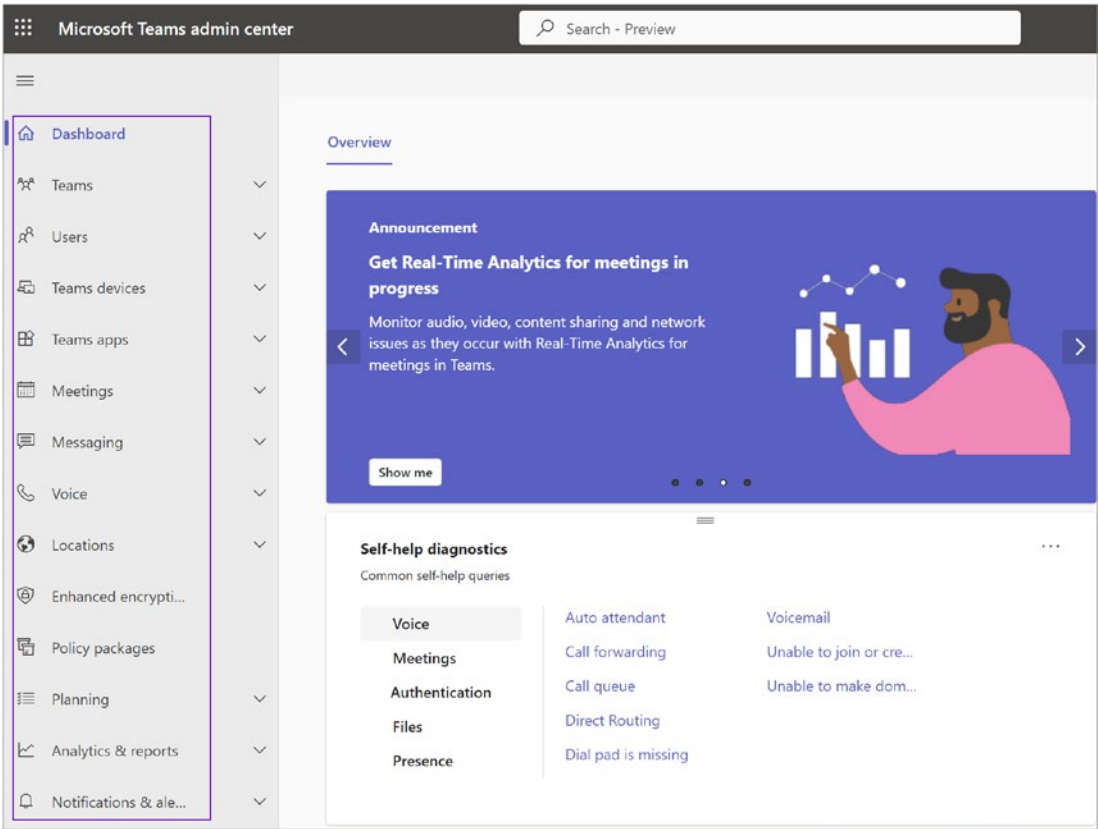


Figure 2-31. Teams admin center dashboard

Admin Center: Teams Tab

The first management tab shown in the Teams admin center is Teams. By using this tab you can manage your organization’s teams and channels that users have created. This includes creating new teams, managing existing ones, setting up team permissions, and even deleting teams when necessary.

Manage Teams

When you click Manage Teams, you will see a global view of the teams that have been created in your organization. As an admin, you can manage every team from this tab. You can also add or create teams. For example, you can see seven teams created in Figure 2-32. To manage Teams, follow these steps:

1. In the left navigation pane, go to Teams ► Manage Teams.
2. Here, you can view all existing teams, their members, privacy settings, and more.
3. Click a team name to view more detailed settings and to modify the team's settings.

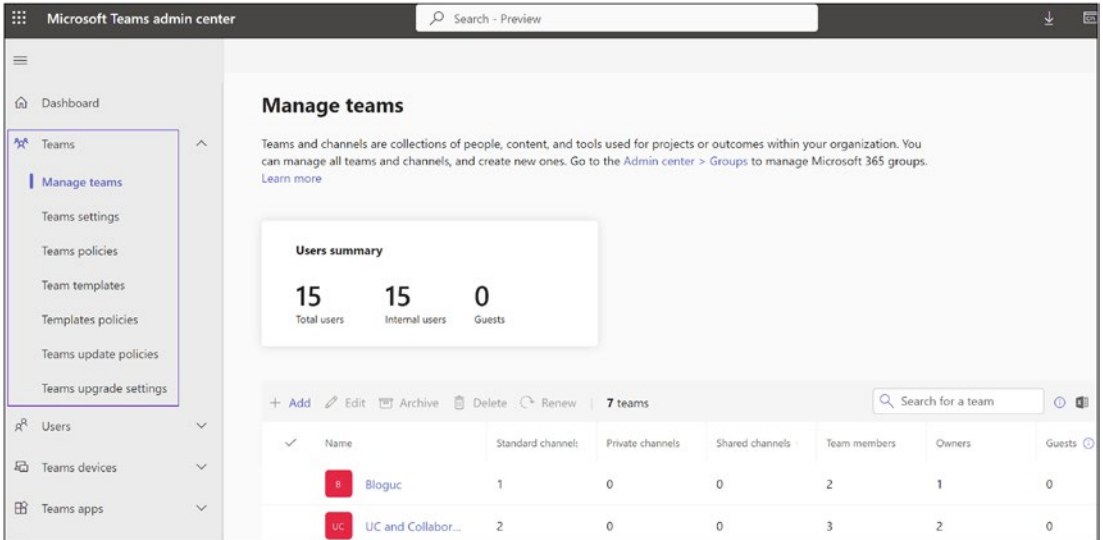


Figure 2-32. The Manage Teams tab

To manage an individual team, click the team name to open a management page for the team. You can add or remove members, modify channels, and change settings. Also, you can edit the team name and description and modify the team's privacy settings. In this example, clicking the Teams Admin Training team displays the management options shown in Figure 2-33.

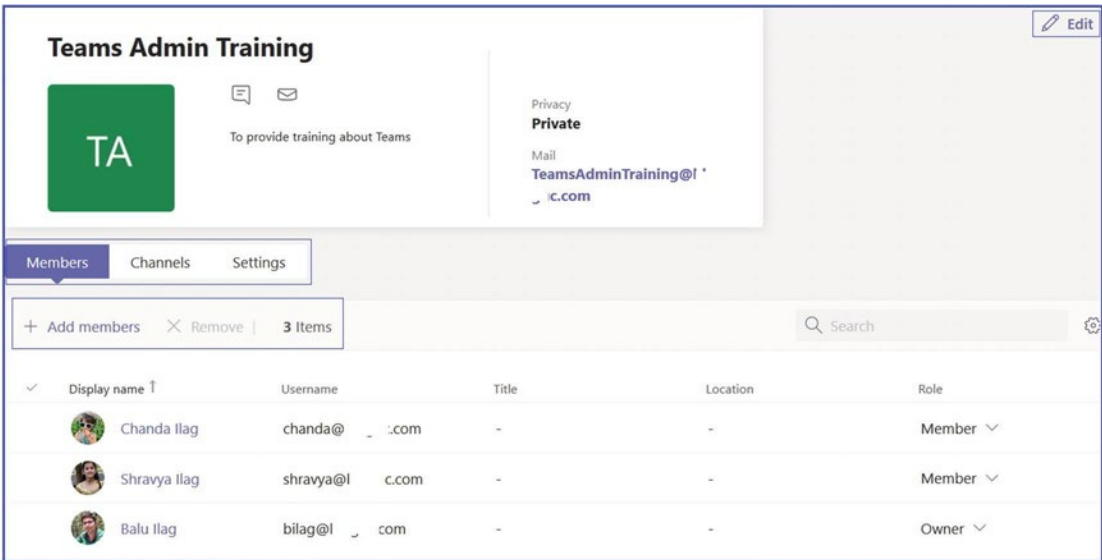


Figure 2-33. Managing a team and channel

Teams Settings

Teams settings allow you to set up your teams for features such as email integration, cloud storage options, and device setup. When you make changes to the Teams settings, they will be applied to all the teams within your organization.

You can enable and manage different organization-wide Teams settings including notifications and feeds, email integration, files, organization, devices, and directory search (search by name). Let’s understand each setting in detail.

Notification and Feeds

The notification and feeds settings allow you to manage the way that Teams handles suggested and trending feeds. Once you enable this setting, users will see the suggested feeds in their activity feeds.

Tagging control how tags are used across your organization. Tags can be added to one or multiple team members and used in @mentions by anyone on the team to notify people who are assigned that tag of a conversation.

To enable notification and feeds, follow these steps:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.

2. Under Notification and Feeds, turn on the “Suggested feeds can appear in a user’s activity feed” option, as shown in Figure 2-34.
3. Under Tagging, set who can manage tags and more.
4. Once you have made the required changes, click Save to commit the changes.

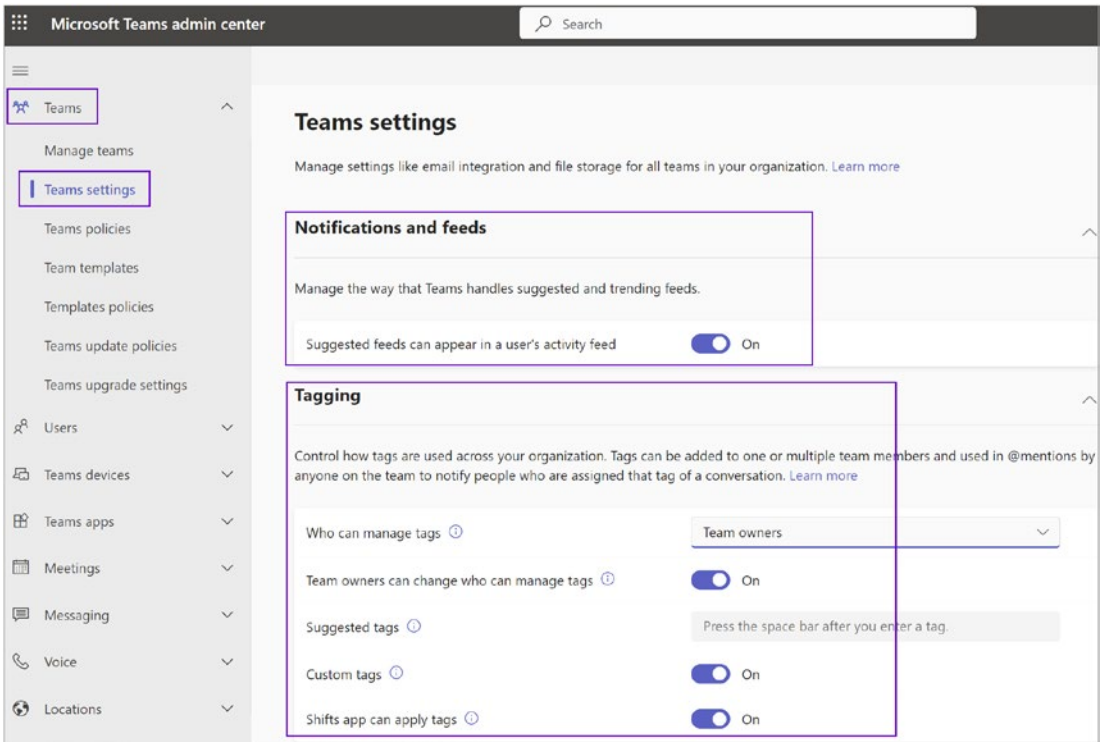


Figure 2-34. Notifications and feeds and tagging

Email Integration

Email integration is one of the most popular integration features among users. You as a Teams admin can use the Teams admin center to configure email integration. This is useful when you are integrating Teams into existing messaging workflows to provide information through email to team members. It is possible to retrieve email addresses for any individual channel within a team. Messages sent to these email addresses are then posted as conversation messages to the conversations of the channel, and other members can download the original message or add comments to the messages content.

Remember, the maximum message length for Teams messages is 24 KB, which can be reached quickly when creating an email. Therefore, if you just want to post basic information into a channel, you should use a text-only email. Otherwise, only the first part of the email is displayed as a team’s conversation, and all team members who want to read the message must download and open it using an electronic mail (EML) format. EML files can contain plain ASCII text for the headers and the main message body as well as hyperlinks and attachments.

Getting an Email Address for a Channel

In Microsoft Teams, any team member can retrieve the email address of channels by clicking the more options (...) icon to the right of a channel’s name and then selecting “Get email address” (see Figure 2-35).

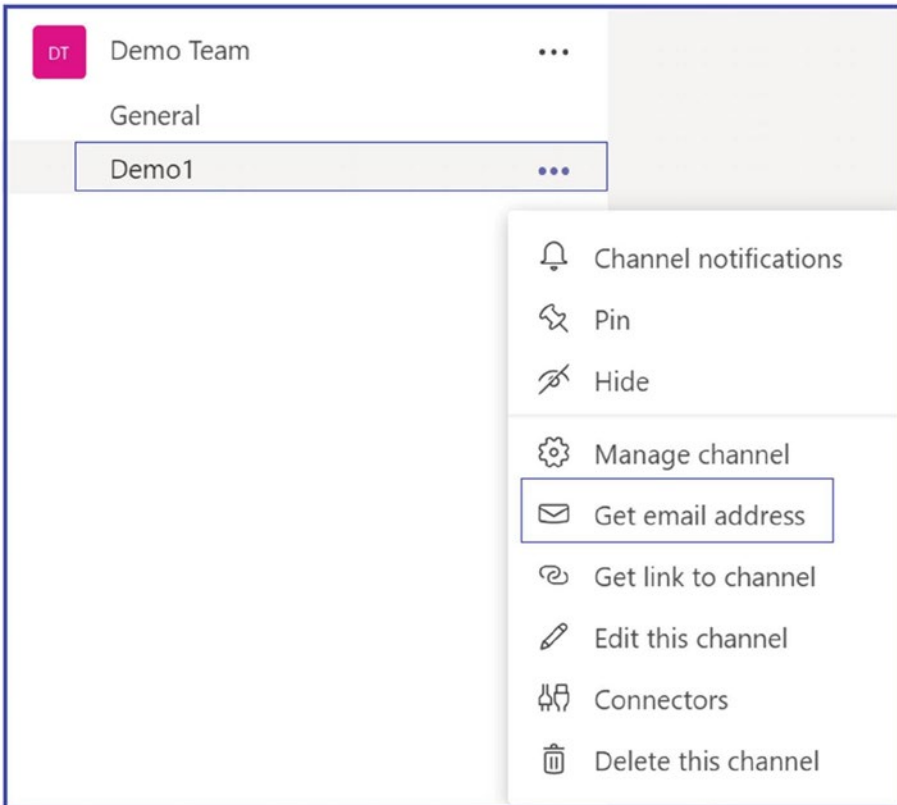


Figure 2-35. Retrieving the email address of a channel

The format of these channel email addresses makes them difficult to recognize because they appear similar to this demo address: ChannelName - TeamName <UniqueID.TenantName.onmicrosoft.com@amer.teams.ms>. Here's an example: Demo1 - Demo Team fb181c9a.bloguc.com@amer.teams.ms.

For ease of management, team owners and users can remove the email address, or they can modify advanced settings to restrict message delivery to team members and certain domains only.

Note When an email is sent to the channel's email address, the email is stored as an EML file in the folder Email Messages in the channel's document library. All participants of a channel can download the files and open them in their preferred viewer for EML files.

Enabling and Managing Email Integration

Email integration lets people send an email to a Teams channel and have the contents of the email displayed in a conversation for all team members to view. This feature is very useful. To enable email integration, follow these steps:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under Email Integration, turn on the "Users can send emails to a channel email address" option.
3. Add the SMTP domains from which channel emails will be accepted. Once you have made the required changes, click Save to commit the changes. As an example, Figure 2-36 shows the bloguc1.com and bloguc2.com SMTP domains added to accept the channel emails.

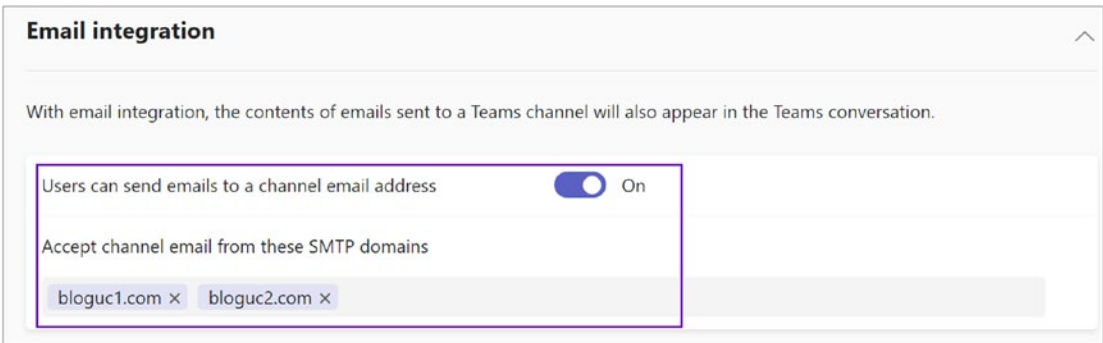


Figure 2-36. *Email integration*

Files (Enabling and Managing File Sharing and Cloud File Storage)

Now that you have learned about the different file storage options Teams uses, to enable file storage, follow this procedure:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under Files, turn on or off the options for Citrix files, Dropbox, Box, Google Drive, and Egnyte.
3. Once you have made the required changes, click Save to commit the changes. As an example, Figure 2-37 shows that the Bloguc organization allows all four types of file storage.

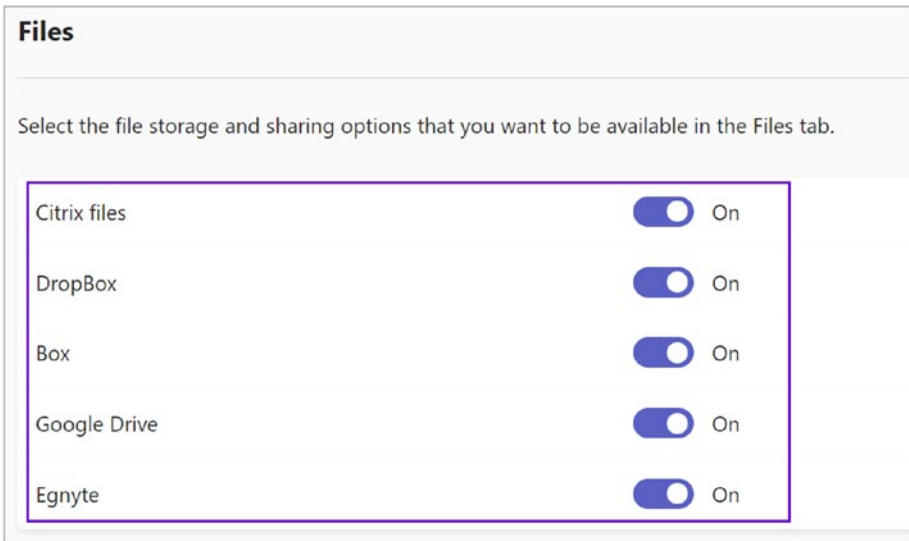


Figure 2-37. Teams settings for files

Organization Settings

In Teams, the Organization tab allows Teams users to see others in their organization's hierarchy. The Show Organization tab in chats allows users to show or hide the Organization tab in chats that shows additional data about a chat partner. An admin can manage enabling or disabling Organization tab details per your organization's requirements. To enable the Organization tab, follow these steps:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under Organization, turn on the Show Organization Tab In Chats option.
3. Once you have made the required changes, click Save to commit the changes. The example in Figure 2-38 shows that the Bloguc organization allows the Organization tab to be displayed in chat.

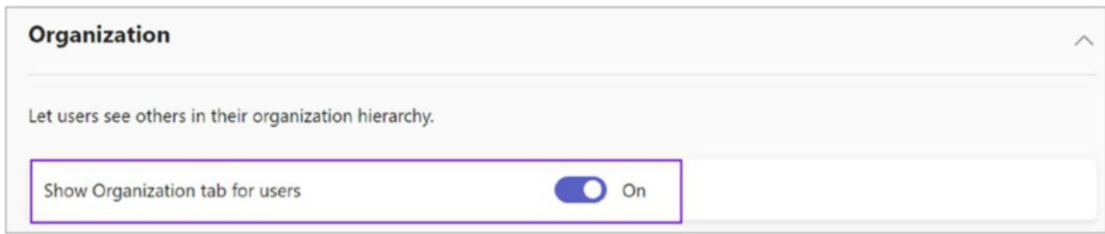


Figure 2-38. Teams settings organization

Devices

Teams provides organization-wide device settings to set up how meeting room devices operate in meetings. There are three different settings.

- *Require a secondary form of authentication to access meeting content:* This setting controls whether users must provide a second form of authentication before entering a meeting. This setting is especially useful when using Surface Hub devices, where users can possibly join a meeting with the identity of a different user who is already logged on. You want this setting to provide an additional security verification before users can access possibly sensitive content. This is especially helpful when using shared devices, such as Surface Hubs, where users often forget to sign off after using a device.
- *Set content PIN:* This setting requires users to enter a PIN before accessing documents from a team. This also is a useful setting for multiuser devices, where users could access the session of a different user who was already logged on. You want to protect access to possibly sensitive content on shared devices, similar to the secondary security verification.
- *Resource accounts can send messages:* This setting allows resource accounts to send messages to participants. You want to allow automatic messages by resources, or you might restrict communication of these accounts. This setting can be helpful when configuring workflows for resources.

To enable devices settings, follow this procedure:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under Devices, select the following settings:
 - a. *Require a secondary form of authentication to access meeting content*: Full Access
 - b. *Set content PIN*: Required For Outside Scheduled Meetings
 - c. *Resource accounts can send messages*: Select On or Off
3. Once you have made the required changes, click Save to commit the changes. As an example, Figure 2-39 shows the Bloguc organization's device settings.

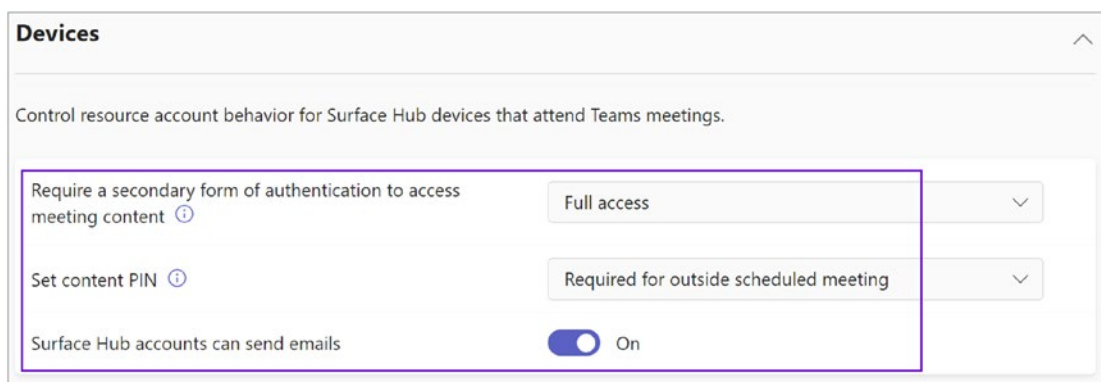


Figure 2-39. Teams settings for devices

Search by Name

Using Microsoft Teams scope directory search, you as an admin can create virtual boundaries that control how users communicate with each other within the organization. Microsoft Teams provides custom views of the directory of organization users. Most important, the Information Barrier policies support these custom views. Once the policies have been enabled, the results returned by searches for other users (e.g., to initiate a chat or to add members to a team) will be scoped according to the configured policies.

Users will not be able to search or discover teams when scope search is in effect. Note that in the case of Exchange hybrid environments, this feature will work only with Exchange Online mailboxes (not with on-premises mailboxes).

To turn on the scope directory search, you need to use Information Barrier policies to configure your organization into virtual subgroups. To configure a scope directory search using an Exchange address book policy in your tenant, follow these steps:

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under Search By Name, turn on the “Scope directory search using an exchange address book policy” option.
3. Once you have made the required changes, click Save to commit the changes. The example shown in Figure 2-40 shows that the Bloguc organization has enabled the scope directory search using an Exchange address book.

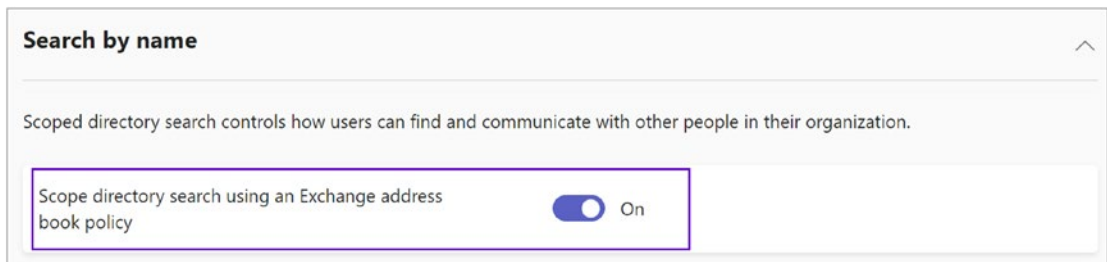


Figure 2-40. Teams setting for a directory search by name

Note If it was not already turned on, you can turn on the scope directory search as a prerequisite to using Information Barrier.

Remember, after enabling scope directory search, before you can set up or define Information Barrier policies, you need to wait at least 24 hours.

Safety and Communications

Role-based chat permissions control the amount of supervision a user needs while chatting with others. Before you turn this on, turn on chat and assign chat permission roles to users.

1. Log in to the Teams admin center, navigate to Teams, and then select Teams Settings.
2. Under “Safety and communications,” turn on the “Role-based chat permissions” option.
3. Once you have made the required changes, click Save to commit the changes. The example shown in Figure 2-41 shows that the role-based chat permission enabled.

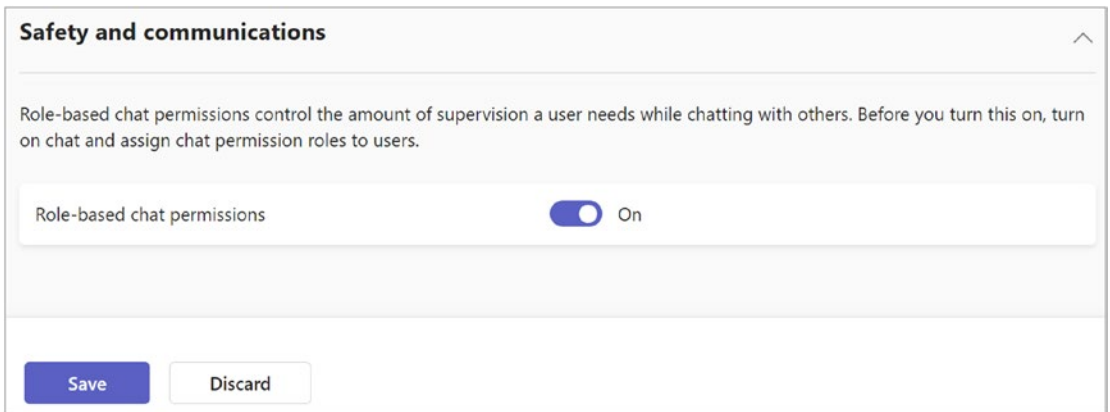


Figure 2-41. Teams “Safety and communications” settings

Best Practices for Email Integration

Channel email addresses are lengthy and contain the Teams domain, which make them difficult to remember. It is a best practice for users to create contact objects for the channel addresses or for Exchange administrators to create mail contacts that provide an easily recognized mail address in their own organization custom domain. For example, `bloguc.com`, for my Demo Team, has few channels. One channel named Demo1 in the team Demo Team has the email address `Demo1 - Demo Team fb181c9a.bloguc.com@amer.teams.ms`.

When you create a mail contact with the alias `demo1-team@bloguc.com` and set its external email address to `123ab345.1.bloguc.onmicrosoft.com@amer.teams.ms`, all email sent from internal users to the preceding email address will be forwarded to the team's channel.

Remember, users can remove and reactivate a channel's email address, in which case a new address is generated, and the old address cannot be reused. This invalidates the mail contact's external address, which in turn must be changed when this occurs.

Teams Policies

Let's talk about Teams policies.

Creating and Managing Teams Policies

Policies in Teams allow you to control what users in your organization can do or cannot do. For instance, you can create meeting policies to control who can schedule or record meetings, messaging policies to control what users can do in private and channel messages, etc.

Another important task you can perform inside Teams is managing Teams policies. Using Teams policies, you can control how teams and channels are used in your organization and what settings or features are available to users when they are using teams and channels. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies for users who are members of a team or a channel within your organization. You can create new a Teams policy or manage the existing Global (Org-wide default) or custom policy.

Creating a New Teams Policy

To create a Teams policy, log in to the Teams admin center, navigate to Teams, and select Teams Policies. Click +Add. Once the new Teams policy form opens, enter a meaningful name and description and turn on or off the discovery of private teams and the creation of channels. Figure 2-42 shows new Teams policy settings.

Microsoft added private channels, so they modified the Teams default policies. By default, anybody in your organization can create a private channel with the exception of guests. This default behavior can be controlled at the tenant level in the Teams Global policy.

- *Create private channels:* Team owners and members with permission can create private channels for a specific group of users in your organization. Only people added to the private channel can read and write messages.
- *Create shared channels:* Team owners can create shared channels for people within and outside the organization. Only people added to the shared channel can read and write messages.
- *Invite external users to shared channels:* Owners of a shared channel can invite external users to join the channel, if Azure AD external sharing policies are configured. If the channel has been shared with an external member or team, they will continue to have access to the channel even if this control is turned off.
- *Join external shared channels:* Users and teams can be invited to external shared channels, if Azure AD external sharing policies are configured. If a team in your organization is part of an external shared channel, new team members will have access to the channel even if this control is turned off.

Admins can modify this behavior and assign custom policy to targeted users to allow or block private channel creation.

Note Consider the increased SharePoint workload before allowing private channel creation for everyone in your organization.

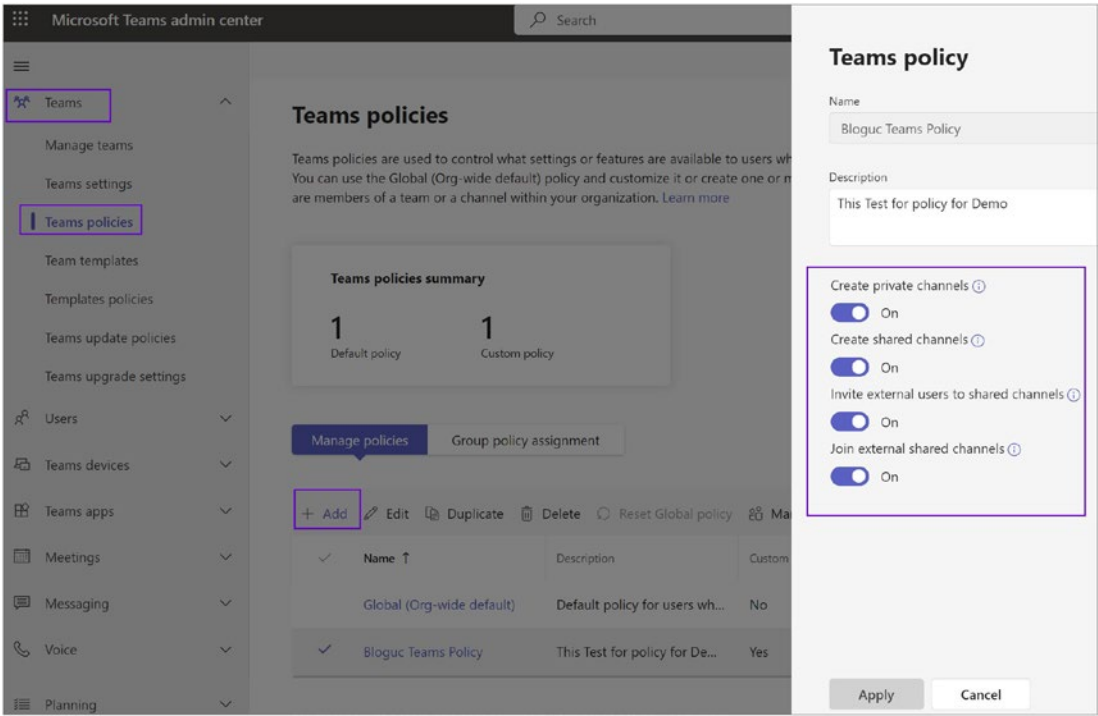


Figure 2-42. Creating a new Teams policy

Teams Templates

Teams templates make it easy to create new teams by providing a predefined template of channels, apps, and settings. You can use the default templates provided by Microsoft or create your own. Refer to Figure 2-43. Users can easily go to the Teams client and create a team using template.

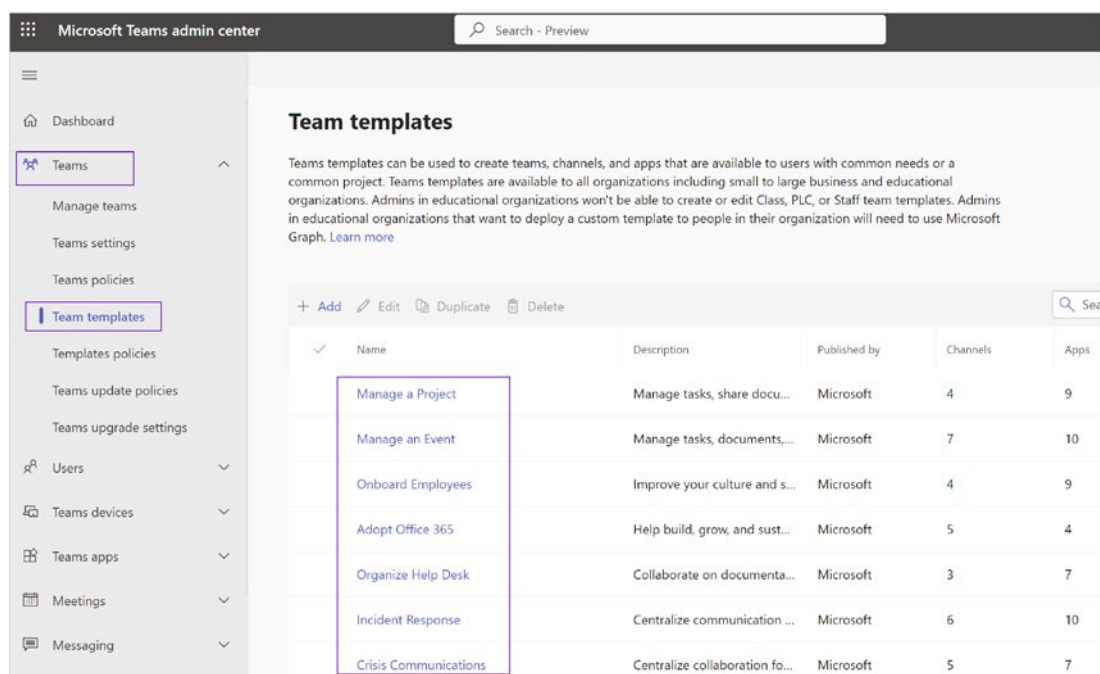


Figure 2-43. Teams templates

You can find details about the predefined templates here:

<https://learn.microsoft.com/en-us/microsoftteams/get-started-with-teams-templates-in-the-admin-console#pre-built-team-templates-in-the-teams-admin-center>

Template Policy

You can set what templates can be seen by users. To hide a template, go to “Template policy,” click Add, select which template you need to hide, and click Hide. We can create multiple policies and assign them to users. In the user policy, you will be able to see the template policy. Also, you can create a new template by clicking the +Add button.

Template Policies

Templates policies let you create and set up policies that control what templates people in your organization can see. You can use the Global (Org-wide default) policy and customize it, or you can create custom policies. Also, you can assign newly created policies to users.

Teams Update Policies

Update policies allow you to control how and when Teams clients get updates. You can create different update policies and assign them to users or groups of users.

To manage update policies, follow these steps:

1. In the left navigation, go to Teams ► Teams update policies.
2. Here, you can view, create, and manage update policies, and assign them to users.

Teams Upgrade Settings

The upgrade settings in the Teams admin center help you control the coexistence and upgrade experience from Skype for Business to Teams. The upgrade organization-wide settings allow Teams admins to set up the upgrade experience from Skype for Business to Microsoft Teams for their organization users. As an admin, you can use the default settings or make changes to the coexistence mode and app preferences to fit your organizational needs. Migrating or moving from Skype for Business (on-premises) to Teams is more than a practical migration. Basically, this move signifies a change in how users communicate and collaborate, and change is not always easy. The perfect upgrade method should address the technical aspects of your upgrade as well as encourage user acceptance and adoption of Teams, driving a positive user experience and business outcome understanding.

For comprehensive migration and upgrade details, refer to Chapter 6. The material here is simply an overview of Teams upgrade settings.

Once you are planning the transition from Skype for Business to Teams, you will need to become familiar with the various upgrade modes, notions, and terminology applicable to upgrading from Skype for Business to Teams. Figure 2-44 shows a default view of the Teams upgrade settings.

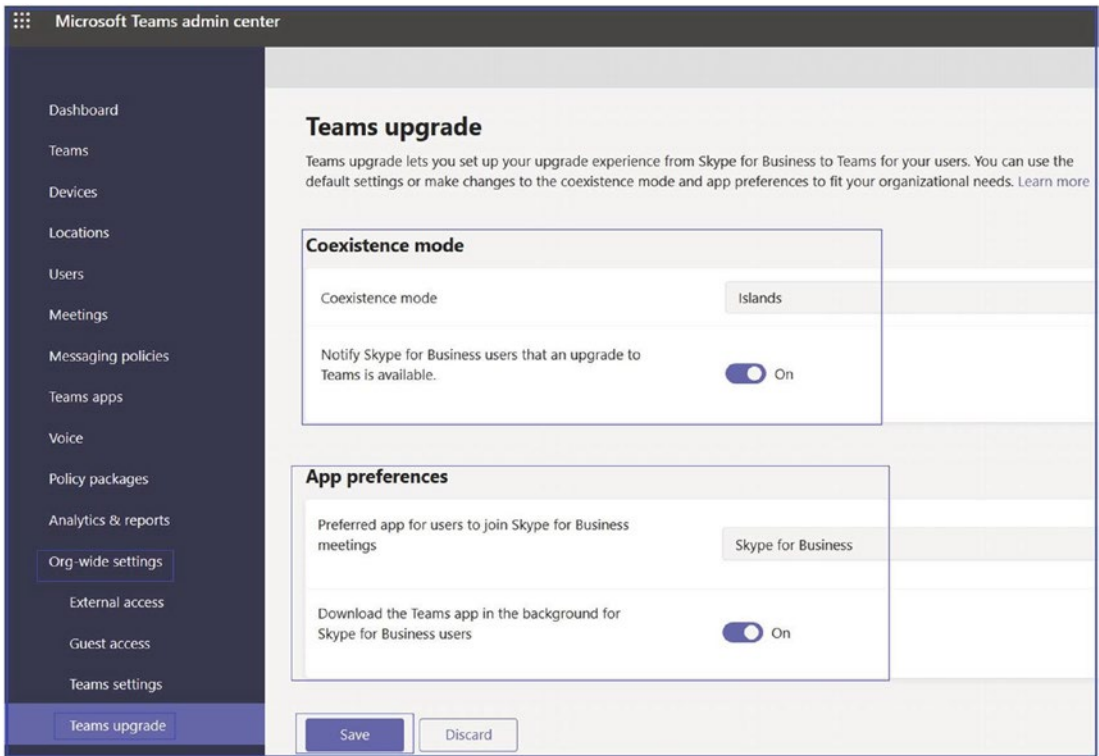


Figure 2-44. Teams upgrade settings

First let's understand the various upgrade modes available in the Teams admin center before making an upgrade plan.

- *Islands mode:* In the Islands upgrade coexistence mode for Teams, every client will use both Skype for Business and Microsoft Teams, operating side by side. The Skype for Business client talks to Skype for Business, and the Microsoft Teams client talks to Teams. Users are always expected to run both clients and can communicate natively in the client from which the communication was initiated.
- *Skype for Business Only mode:* Using this Teams upgrade coexistence mode, users continue using Skype for Business as they are, and there are no Teams capabilities allowed such as chat, meeting, and calling capabilities. They do not use Teams for teams and channels. This mode can be used prior to starting a managed deployment of Teams to prevent users from starting to use Teams ahead of their readiness.

This can also be used to enable authenticated participation in Teams meetings for Skype for Business users, if the users are licensed for Microsoft Teams.

- *Skype for Business with Teams collaboration (SfBWithTeamsCollab) mode:* In this upgrade mode, Skype for Business continues to support chat, calling, and meeting capabilities, and Microsoft Teams is used for collaboration capabilities such as teams and channels, access to files in Office 365, and added applications. Teams communications capabilities, including private chat, calling, and scheduling meetings, are off by default in this mode. This mode is a valid first step for organizations still relying on Skype for Business that want to provide a first insight into the collaboration capabilities of Teams for their users.
- *Skype for Business with Teams collaboration and meetings (SfBWithTeamsCollabAndMeetings) mode:* In this mode, private chat and calling remain on Skype for Business. Users will use Teams to schedule and conduct their meetings along with team- and channel-based conversations in this mode. This mode is also known as Meetings First mode. This coexistence mode is especially useful for organizations with Skype for Business on-premises deployments with Enterprise Voice, who are likely to take some time to upgrade to Teams and want to benefit from the superior Teams meetings capabilities as soon as possible.
- *Teams Only:* In this mode, a Teams Only user (also called an *upgraded user*) has access to all the capabilities of Teams. They might retain the Skype for Business client to join meetings on Skype for Business that have been organized by nonupgraded users or external parties. An upgraded user can continue to communicate with other users in the organization who are still using Skype for Business by using the interoperability capabilities between Teams and Skype for Business (if these Skype for Business users are not in Islands mode). However, an upgraded user cannot initiate a Skype for Business chat, call, or meeting. As soon as your organization is ready for some or all users to use Teams as their only communications and collaboration tool, you can upgrade those users to Teams Only mode.

Note Even if the Skype for Business Only mode is meant to have the collaboration features of Teams disabled, in the current implementation, teams and channels are not automatically turned off for the user. This can be achieved by using the App Permissions policy to hide teams and channels.

Figure 2-45 shows details for all five upgrade modes.

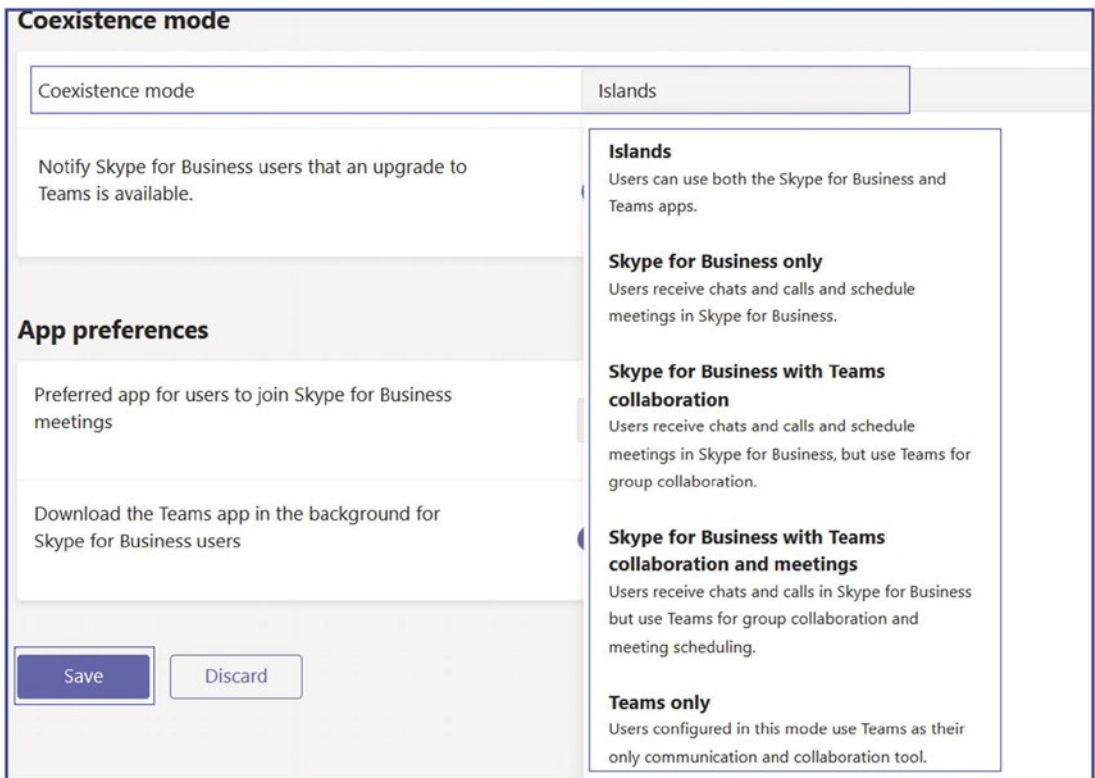


Figure 2-45. Teams coexistence modes

Setting Teams Upgrade Mode

Before enabling Teams upgrade mode for users, you as an admin must undertake extensive planning and preparation, including the readiness of network infrastructure to allow Teams media traffic, the setup of your firewall to allow Teams traffic seamlessly, the Teams client deployment, and adoption. Once you are ready for the changeover from

Skype for Business to Teams, you will need to choose the appropriate upgrade path and coexistence modes for a smooth transition to Microsoft Teams in your organization.

You can use the same coexistence mode for all the users and upgrade to Microsoft Teams all at once, or you can do the migration by region, site, or group by configuring different coexistence modes for different groups of users.

To set the coexistence mode for your organization’s users, follow these steps:

1. Log in to Microsoft Teams admin center, and then navigate to Teams. Select Teams Upgrade Settings.
2. On the Teams upgrade page, from the Coexistence mode options, select one of the following options for your organization users:
 - Islands
 - Skype For Business Only
 - Skype For Business With Teams Collaboration
 - Skype For Business With Teams Collaboration and Meetings
 - Teams Only
3. Under Coexistence Mode, you can enable the “Notify Skype for business users that an upgrade to Teams is available” without selecting Teams Only mode.
4. Then under App Preferences, you can select the preferred app for users to join Skype for Business meetings. I recommend using the Skype meeting app for seamless joining.
 - Skype Meetings App
 - Skype For Business
5. Turn on the “Download the teams app in the background for Skype for business users,” which will download the Teams app on their machine.
6. Click Save to save the changes.

Note Microsoft has announced that all new Office 365 tenants are onboarded directly to Microsoft Teams for chat, meetings, and calling. Therefore, you will not see the options to select a coexistence mode if you have a newly provisioned tenant.

Setting Upgrade Options for an Individual User Using the Teams Admin Center

You learned about the Teams coexistence modes and how to enable an upgrade mode for a whole tenant, but what if you want to set different coexistence modes for different users? This can be achieved through the Teams admin center. To set a coexistence mode for an individual user, follow these steps:

1. Log in to the Microsoft Teams admin center and then navigate to and select Users. Locate the user for whom you would like to set the upgrade options. For this example, I have selected Chanda Ilag as the user to whom to assign a coexistence mode.
2. On the user page, on the Account tab, under Teams Upgrade, click Edit.
3. In the Teams Upgrade window, select one of the following options for the selected user:
 - Use Org-wide Settings
 - Islands
 - Skype For Business Only
 - Skype For Business With Teams collaboration
 - Skype For Business With Teams collaboration And Meetings
 - *Teams Only*
4. At the end, click Apply. The example in Figure 2-46 shows Teams Only assigned to user Chanda Ilag.

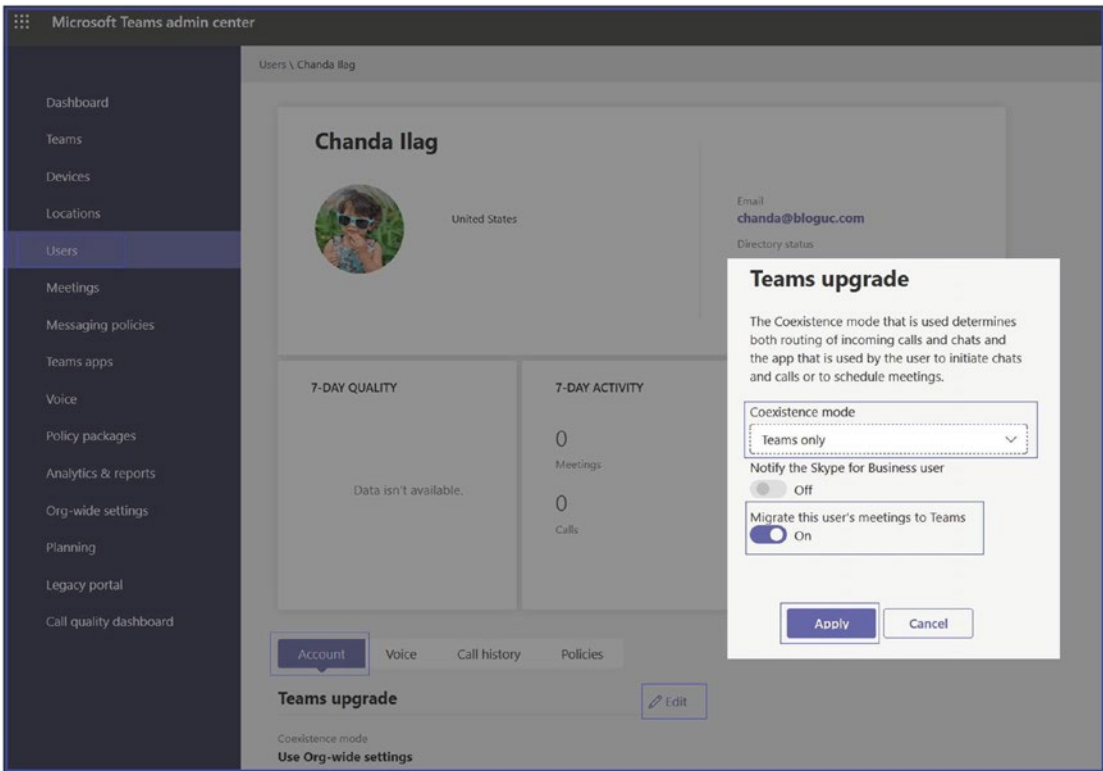


Figure 2-46. Assigning a Teams upgrade mode

Note If you select any coexistence mode (except Use Org-wide Settings), you will have the option to enable notifications in the user’s Skype for Business app, which will inform the user that the upgrade to Teams is coming soon. Enabling this for the user is done by turning on the “Notify the Skype for business user” option.

Selecting Teams Upgrade Mode Using PowerShell

As a Teams admin, you can use Windows PowerShell to assign a Teams coexistence mode to users. PowerShell is a decent option for automation as well. To manage the transition from Skype for Business to Teams, you can use the `Grant-CsTeamsUpgradePolicy` command, which enables admins to apply `TeamsUpgradePolicy` to

individual users or to configure the default settings for an entire organization. For example, to configure the user `chanda@bloguc.com` to Teams in `SfBWithTeamsCollab` mode and to notify the user, run the following command:

```
Grant-CsTeamsUpgradePolicy -PolicyName SfBWithTeamsCollabWithNotify  
-Identity "chanda@bloguc.com"
```

Another example is to configure a `TeamsOnly` policy for the entire organization by running the following command:

```
Grant-CsTeamsUpgradePolicy -PolicyName TeamsOnly -Global
```

The next example shows how to remove a Teams upgrade policy:

```
Grant-CsTeamsUpgradePolicy -PolicyName $null -Identity chanda@bloguc.com
```

Admin Center: Users Tab

The Users tab within the Microsoft Teams admin center is a one-stop portal for managing individual users and their corresponding settings. Let's delve deeper into its key functionalities including managing users, regulating guest access, and controlling external access.

As an admin, most of your time will be spent managing users. In the Teams admin center, the Users tab allows you to manage all your users with different settings such as audio conferencing settings, the policies assigned to them, phone numbers, and other features for users in your organization who use Teams. Figure 2-47 shows a list of users and their different settings.

If you want to manage other user settings, such as by adding or deleting users, changing passwords, or assigning licenses, you need to visit the Office 365 admin center and navigate to Users.

User Management

The User Management function empowers admins to handle a myriad of settings, policies, and functionalities for each individual within the organization. To begin managing users, navigate to the Microsoft Teams admin center, select Users, and then Manage Users.

Here, you can take charge of several user-related tasks such as adding or deleting policies, assigning phone, check user-specific call analytics, and more. Additionally, you can handle audio conferencing settings, allocate phone numbers, and manage various Teams policies for each person.

Essentially, this section ensures you have full control over user-level features and functionalities.

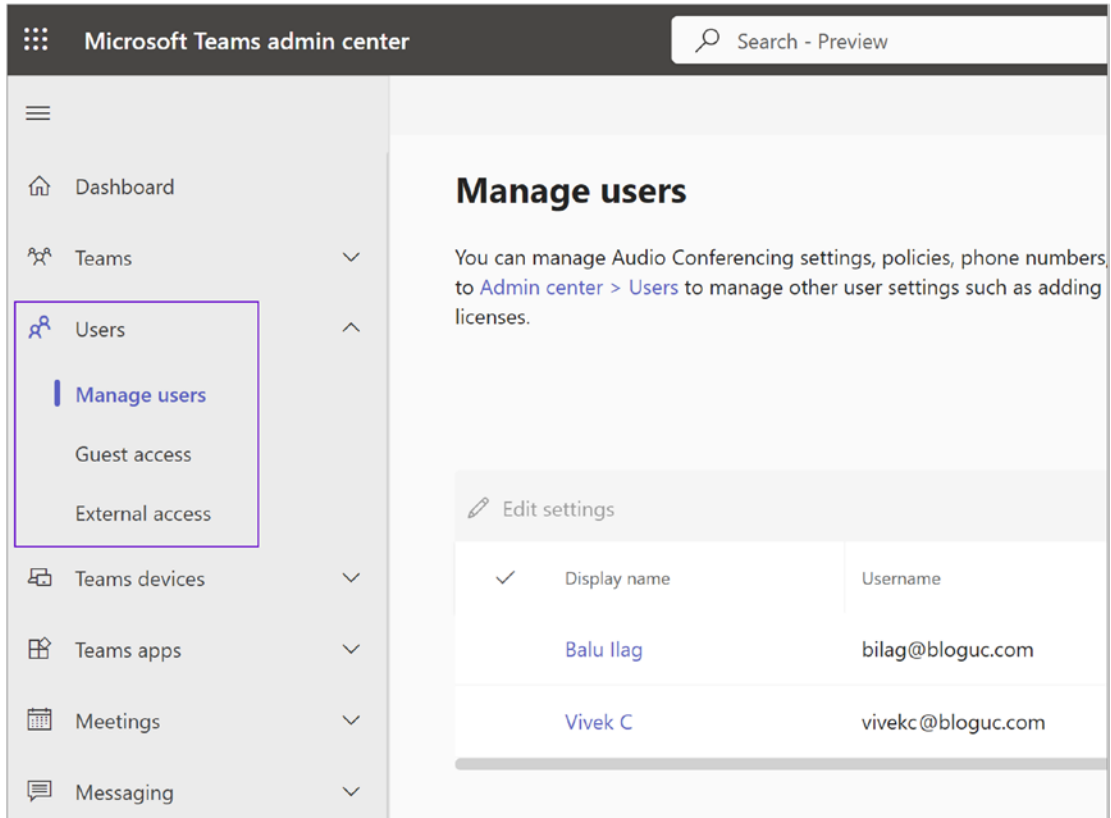


Figure 2-47. Users and their different settings

Guest Access

With guest access, you can regulate how guests interact and collaborate with your organization’s users. This feature allows you to extend an invitation to individuals outside your organization, granting them access to specific teams. These guests can join meetings and engage in chats with your users. The guest access feature provides a controlled environment for external collaboration, while keeping your data secure.

Microsoft Teams offers external collaboration through two methods: guest access and external access, also known as federation access. We already learned about external access, so now we will cover guest access in detail.

Guest access permits teams in your organization to work together with users outside your organization by allowing them access to existing teams and channels on one or more of your tenants. Someone with an organization or consumer email account, such as Outlook, Hotmail, Gmail, or any other domain, can participate as a guest in Teams with full access to team chats, meetings, and files. Guest access is an org-wide setting in the Teams admin center and is turned off by default. Allowing guest access in Teams requires guest access in Teams, Azure AD, and Office 365 services. Before guest access is allowed and users add guests in their teams, as an admin you need to secure the environment so that guests will get specific access to what they need, not full access to everything.

The formal definition of guest access is access for users or individuals who do not have identity in your organization. For example, in the Bloguc.com organization, a user added `abc@microsoft.com` to their team as a guest. That means a Microsoft user is added to the Bloguc organization as a guest. The guest organization (Microsoft) will control the authentication layer, and the Bloguc organization controls the authorization layer that determines what the guest can access.

Don't confuse external access and guest access. Guest access gives access permission to an individual. External access gives access permission to an entire domain. Guest access uses your existing licenses when using certain features. Teams doesn't restrict the number of guests you can add. However, the total number of guests that can be added to your tenant is based on what your Azure AD licensing allows, typically five guests per Azure AD licensed user. External access allows you to communicate with users from other domains that are already using Teams. Therefore, they need to provide their own licenses to use Teams.

Adding Guest Users in Microsoft Teams

When a guest user wants access, they first need to get invited through email or invited/added in Azure as a guest user. Once the guest user accepts the invite, they get added to Azure AD in the cloud only. Remember, there is no on-premises data access. An invited guest account is not governed because there is no password to maintain. Guest authentication happens through its own tenant because it is federated with the Office 365 tenant.

Other than Azure AD tenants, a user like Google (Gmail) can also get invited for guest access. Once they are accepted and sign in to Gmail, no secondary authentication is required. Office 365 gets federated to that organization. Pretty much everything that is based on Security Assertion Markup Language (SAML) or Web Service (Ws)-federated is permitted to have guest access in Teams. Guest authentication is therefore managed by the guest's own organization tenant, and access is governed done by Teams, where the users gets specific access as a guest user.

Enabling and Managing Guest Access in Teams

As an admin, you can add guests in your tenant, and you can manage their access as well. As a security and Teams administrator, you have the capability to disable or enable guest access for Teams using the Teams admin portal and Windows PowerShell with the Teams service administrator role permission or global admin permission.

You can add guests at the tenant level, set and manage guest user policies and permissions, and view reports on guest user activity. These controls are available through the Microsoft Teams admin center. Guest user content and activities are under the same compliance and auditing protection as the rest of Office 365.

Note Even if you activate guest access in Teams, you have to make sure that guest access is enabled in Azure AD and SharePoint as well.

Guest access is enabled and managed via four separate levels of permissions. All the authorization levels apply to your Office 365 tenant. As mentioned previously, every authorization level controls the guest experience, as demonstrated here:

- *Azure AD:* Guest access in Microsoft Teams depends on the Azure AD business-to-business (B2B) platform. This authorization level controls the guest experience at the directory, tenant, and application levels.
- *Office 365 groups:* This controls the guest experience in Office 365 Groups and Microsoft Teams.

- *Microsoft Teams*: This controls the guest experience in Microsoft Teams only.
- *SharePoint Online and OneDrive for Business*: This controls the guest experience in SharePoint Online, OneDrive for Business, Office 365 Groups, and Microsoft Teams.

An admin has the flexibility to set up guest access for organization tenant. For example, if you don't want to allow guest users in Microsoft Teams but want to allow them in general in your organization, such as for SharePoint or OneDrive for Business, just turn off guest access in Microsoft Teams. In another scenario, you could enable guest access at the Azure AD, Teams, and groups levels, but then disable the adding of guest users on selected teams that match one or more measures, such as a data classification of confidential. SharePoint Online and OneDrive for Business have their own guest access settings that do not rely on Office 365 Groups.

Note Theoretically a guest user is a new user object in your Azure AD tenant. On the first line, you can allow or restrict the creation of new guest objects in your tenant, and then you can control whether guest access is allowed or if there are additional dependencies to access different locations, such as Teams, Office 365 Groups, and SharePoint.

Any guest access setting changes could take 2 to 24 hours to take effect, so be patient when you modify any org-wide settings.

You can also use Windows PowerShell commands to set up guest access in Teams. Remember, for Teams settings, you have to use the Skype for Business Online PowerShell module with Teams service admin or global admin permission. The most used and useful command for guest access is `Set-CsTeamsClientConfiguration`.

Open Windows PowerShell and connect to the Skype for Business Online tenant and run commands to enable various levels of guest access in Teams. To allow guest users globally, run the following command:

```
Set-CsTeamsClientConfiguration -AllowGuestUser $True -Identity Global
```

To allow private calling for guests, run this command:

```
Set-CsTeamsGuestCallingConfiguration -Identity Global -AllowPrivateCalling  
$false
```

To allow Meet Now for guests, run the following command:

```
Set-CsTeamsGuestMeetingConfiguration -Identity Global -AllowMeetNow  
$false -AllowIPVideo $false
```

To allow messaging settings like memes for guests, run this command:

```
Set-CsTeamsGuestMessagingConfiguration -AllowMemes $False
```

If you want to limit guest user capabilities in a subset of teams, you can use the Microsoft Teams PowerShell module and the `Set-Team` command. This lets you configure the same limitations as the Teams admin center, but instead of restricting it for all teams, you can focus on a single team. This can be useful if you need to create a team for your external consultants to exchange information without disrupting the existing structure.

Managing Guest Access Setting

As a Teams admin, you can enable and disable guest access settings, manage calling settings for guests, manage what meeting features are available to guests during meetings hosted by people in your organization, and manage messaging features for guests in channel conversations and chats. Figure 2-48 shows the guest access settings and what to enable.

Note Admin can enable or disable guest access permission based on your requirements.

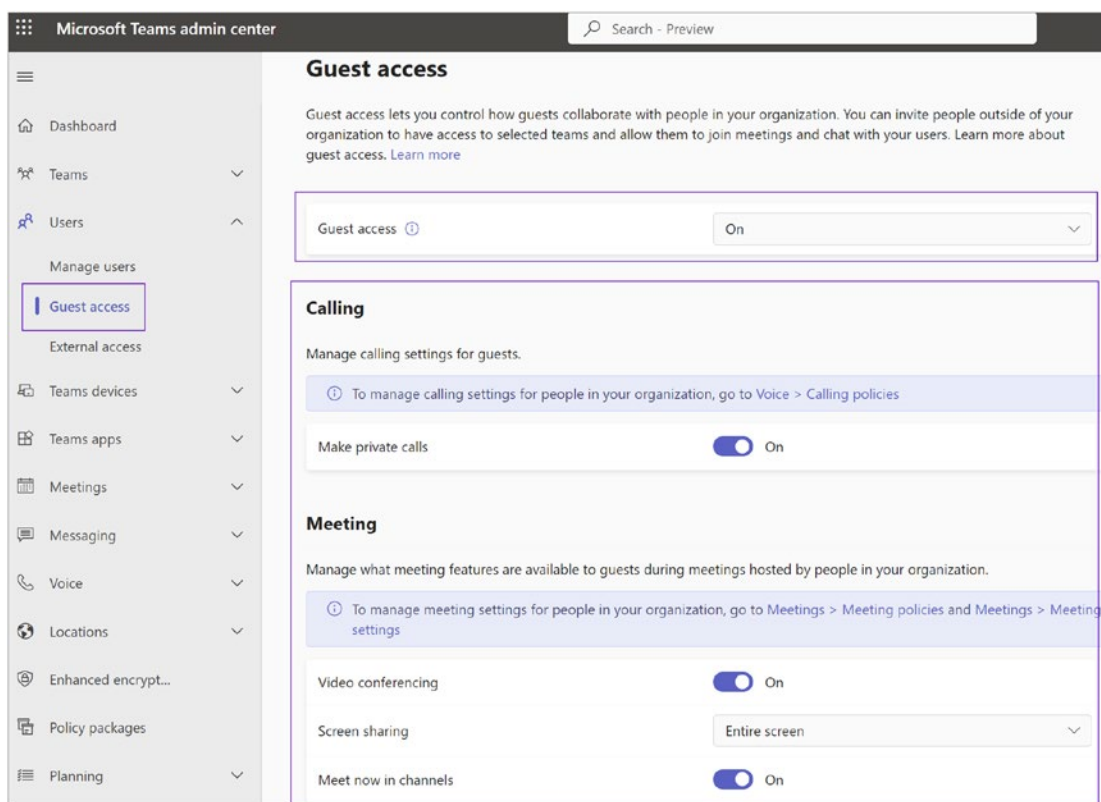


Figure 2-48. Guest access settings

External Access

External access (federation) in Microsoft Teams allows your Teams users to communicate with users who are outside of your organization. By using external access, your users can send messages to or receive messages from users in specific external domains.

Note External (federation) access always uses peer-to-peer sessions; it is not used for group chat or team or channel conversations.

For example, bob@microsoft.com and balu@bloguc.com are working together on a project, and their organizations' other users are also working with each other using their individual Teams account through external access.

Both guest access and external access are used for Teams collaboration both within and outside of your organization. This external collaboration extends the boundaries of Teams to external organizations.

As an admin, you can enable external access for your organization. Before designing external access for your organization, however, understand the different options for setting up external access.

The first option is to enable external access without any restriction (this was called Open federation in Skype for Business). This is the default setting, and it lets people in your organization find, call, and send instant messages and chats, as well as set up meetings with people outside your organization. When you use this setting, your users can communicate with all external domains that are running Teams or Skype for Business and are using Open federation or have added your domain to their allowed list.

The second option allows you to add one or more domains to the allow list. To do this, click Add A Domain, enter the domain name, click Action to take on this domain, and then select Allowed. It is important to know that if you do this, it will block all other domains.

The third option is adding one or more domains to the block list. To do this, click Add A Domain, enter the domain name, click Action to take on this domain, and then select Blocked. It is important to know that if you do this, it will allow all other domains.

Here's how you can use external access in Teams:

- **Communicate across domains:** External access allows your Teams and Skype for Business users to communicate with other users that are outside of your organization.
- **Chat and calling:** Your users can engage in one-on-one chats and make calls with users in the external domain.
- **Share files:** While you can't directly share files with external users in a chat, you can share files from your Teams with external users if they are added as guests to the Team.

- **Participate in Teams:** External users can't be added to Teams, but they can participate in Teams as guests if they have a Microsoft 365 or Office 365 account.

This function allows your users to add apps when hosting meetings or chats with external participants. Simultaneously, your users can utilize third-party apps shared by external participants when they partake in externally hosted meetings or chats.

It's important to note that the data policies of the hosting user's organization, along with the data sharing practices of any third-party apps shared by that user's organization, will be applied in such interactions. Figure 2-49 shows external access settings. In the external access setting page, the admin can customize the settings based on their organization requirements; the available settings are to allow all external domains, add a specific domain and block all external domains, block only specific domains, or block all external domain settings.

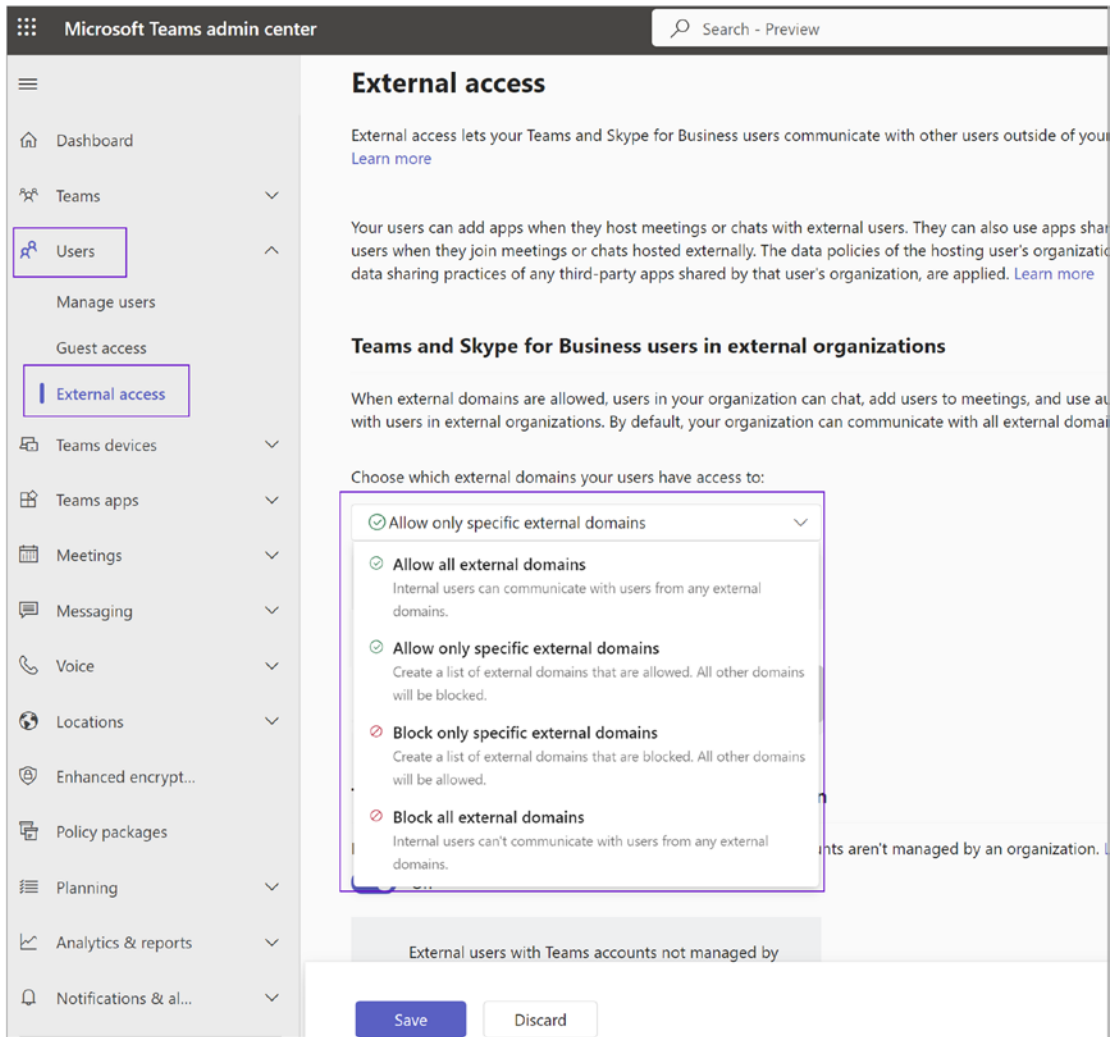


Figure 2-49. External access settings

In essence, the Users tab in the Teams admin center gives you extensive control over user settings, enhancing your ability to manage a safe and productive Teams environment. By understanding and utilizing these functionalities, you can create a customized and secure collaborative space for both your internal users and your external guests.

Admin Center: Teams Devices Tab

Let’s explain the Devices tab.

Managing and Deploying a Teams Phone Endpoint

Microsoft Teams Phone is a flexible telephony solution that seamlessly integrates with Microsoft Teams, enabling users to make and receive calls on various devices such as IP phones, conference phones, or Teams Rooms devices. To efficiently manage and deploy these phone endpoints, administrators can use the Teams admin center.

Microsoft Teams has clients available for the desktop (Windows and macOS), mobile platforms (Android and iOS), Linux clients, and web clients. The end user using Teams on any of these devices will have the same experience. Apart from desktop, mobile, and web clients, there are different devices available that support Teams, such as desk phones, conference rooms, and common area phones. Teams does have native Teams phone and conference rooms available that you can use in meeting rooms and common areas. However, you need to set up a resource account for these room devices.

Store

When navigating a Teams device, the first thing you notice is the store. This is a Teams-certified device store. From here the admin can purchase new devices. Figure 2-50 shows the Teams device store.

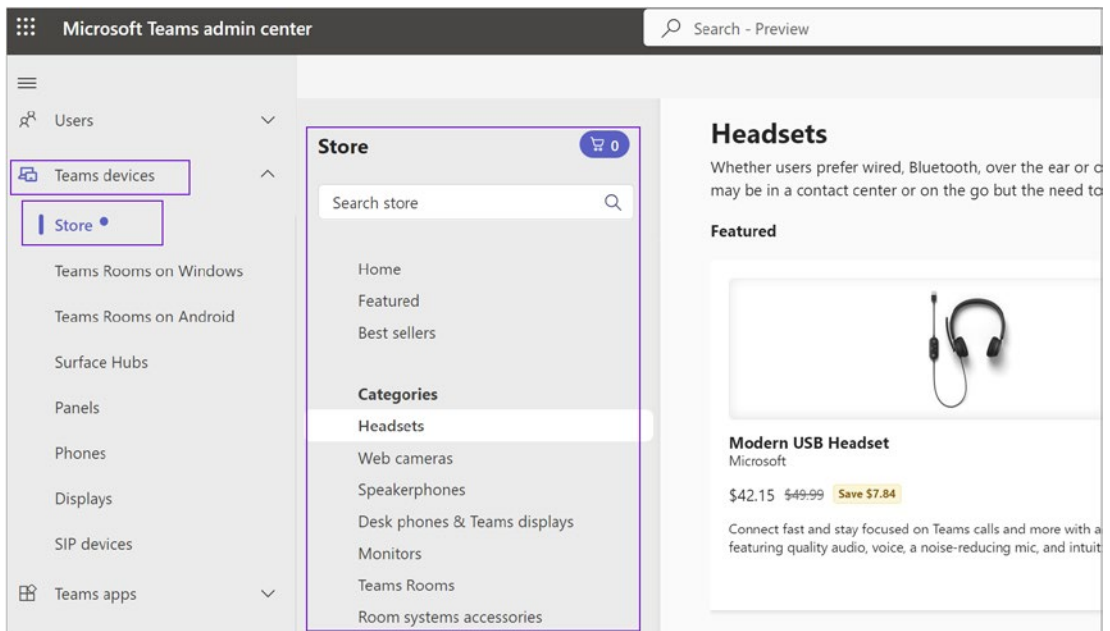


Figure 2-50. Teams device store

Teams Room on Windows

The next device type is the team room on Windows. As a Teams device admin, you can control and manage team rooms on Windows devices such as consoles, microphones, cameras, and displays, in your organization. You can configure settings, view activity information, manage updates, set up alert rules, and perform diagnostics to help with troubleshooting. You will see the status for each device. Figure 2-51 shows the Teams Rooms on Windows page, where the admin can manage them.

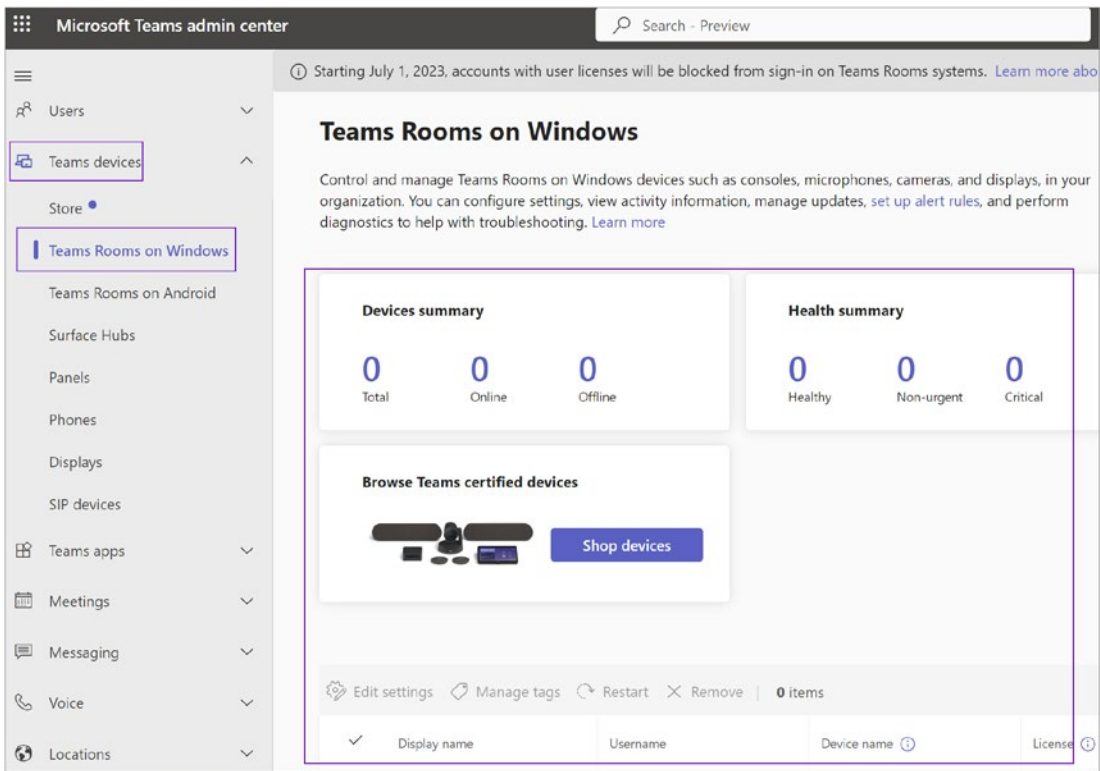


Figure 2-51. Teams Rooms on Windows page

Teams Room on Android

The next device type is the Teams room for Android devices; the admin can control and manage Teams-certified team rooms on Android devices across their organization, create and upload configuration profiles to make changes, set up alert rules, and apply updates for each device.

Surface Hubs

Another device type is Surface Hubs. This offers an all-in-one digital whiteboard, meetings platform, and collaborative computing experience. The Teams device admin can manage Surface Hubs from the Surface Hubs page.

Panels

The next device type is Panels. These types of devices are mounted outside of conference rooms, typically next to room entrances. They show room availability, room name, and reservations. Figure 2-52 shows Panels page, where the admin can manage Teams panel devices.

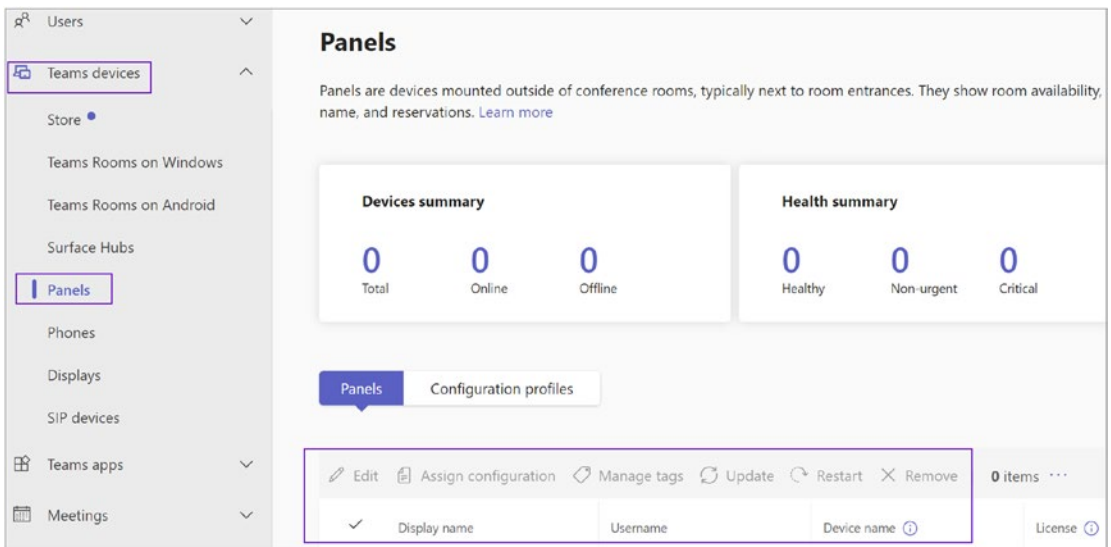


Figure 2-52. Teams Panels page

Phones

The next device type is Phones. As an admin, you control and manage Teams-certified phones across your organization, create and upload configuration profiles for each type of phone you have, make changes to their settings, set up alert rules, and apply software updates.

You will see all the phone devices under Phones such as user phones, common area phones, and conference phones. Additionally, you can create a configuration profile that is assigned to phone devices. Figure 2-53 shows the Teams Phones page, where the admin can manage Teams phone devices.

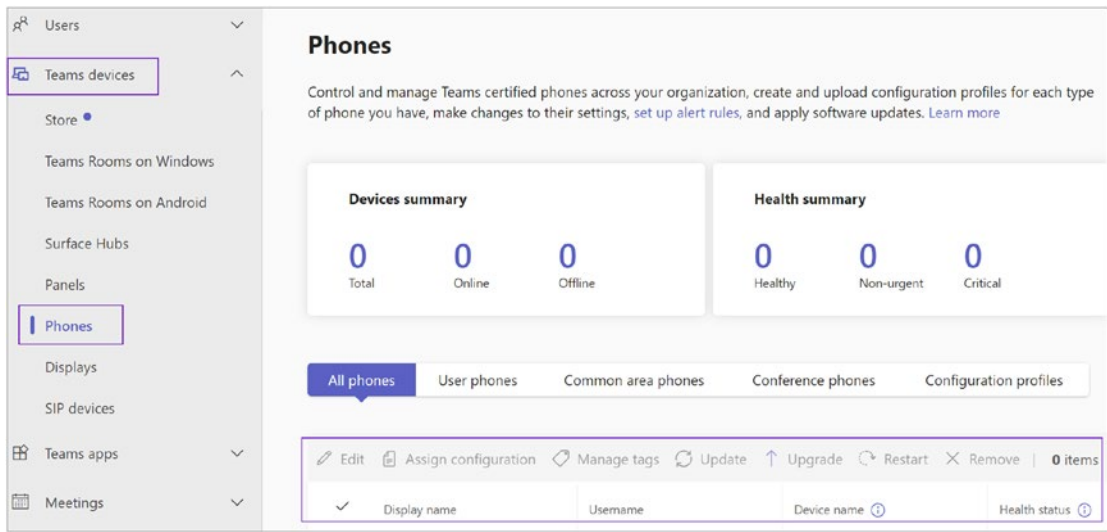


Figure 2-53. Phone devices in the Teams admin center

Displays

On the Display tab, you can manage display devices in your organization, create and upload configuration profiles so you can make setting changes, set up alert rules, and apply updates for each type of device.

SIP Devices

On the SIP Devices tab, you can control and manage Teams-certified SIP devices across your organization.

Creating and Managing Configuration Profiles in Teams

Admins can create and assign configuration profiles to a device or groups of devices to manage them. Device management settings include device status, device updates, restart, monitor diagnostics for devices, and device inventory. These are all management tasks that admins can perform using the Teams admin center.

To manage settings and features for Teams devices in your organization, you can use configuration profiles. As an admin, you can create or upload configuration profiles to include settings and features that you would like to enable or disable and then assign a profile to a device or groups of devices. To set up a profile, you need to create a profile configuration with custom settings, such as general setting with device lock setting,

language, time/date format, time daylight saving, device setting with display screen saver, office hours for device, and network setting with DHCP enabled, hostname, IP address, subnet mask, DNS, and gateway.

Note Out of the box there will no configuration profiles. Admins have to create configuration profiles to assign profiles to devices or groups of devices.

Creating a Configuration Profile to Manage Devices

To create a configuration profile, follow these steps:

1. Log in to the Microsoft Teams admin center. In the left navigation pane, select Teams Devices and click Phones.
2. On the Phones page, select Configuration Profiles, and then click Add.
3. On the Devices/New page, enter the name of the configuration profile and an optional description. Assign a meaningful name so that the profile configuration can be easily identified.
 - a. In the General section, select if you will enable Device Lock and PIN, Language, Timezone, Date Format, and Time Format. Figure 2-54 shows a sample configuration.

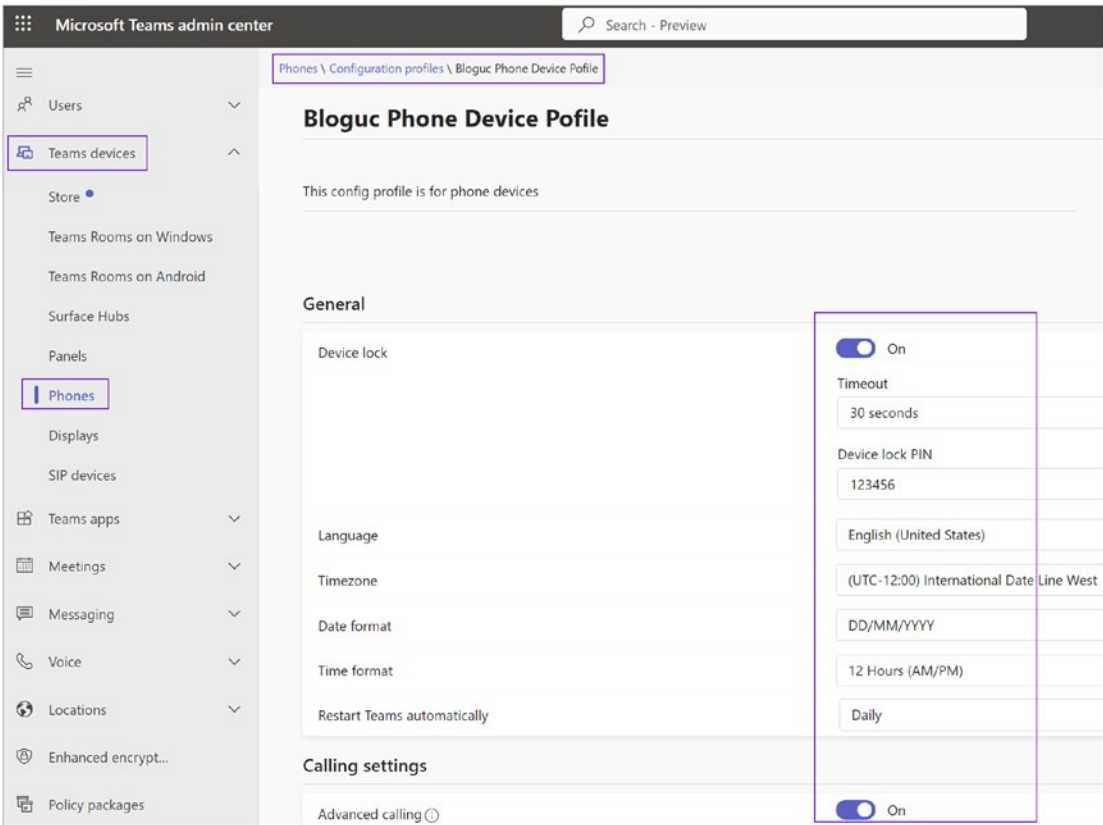


Figure 2-54. Phone configuration

- b. Licensing for common area devices was expanded to include some new features (voicemail, call-forward settings, call park, call queues, auto attendants, Intune enrollment into Endpoint Manager). As you can probably imagine, the basic default common area phone user interface is not going to give you the flexibility to use all these features. Figure 2-42 shows the calling setting option with the advanced calling feature.
- c. In the Device Settings section, select whether you will enable the display of a screen saver, brightness, backlight timeout, contrast, silent mode, office hours, power saving, and screen capture. Figure 2-55 shows sample device settings.

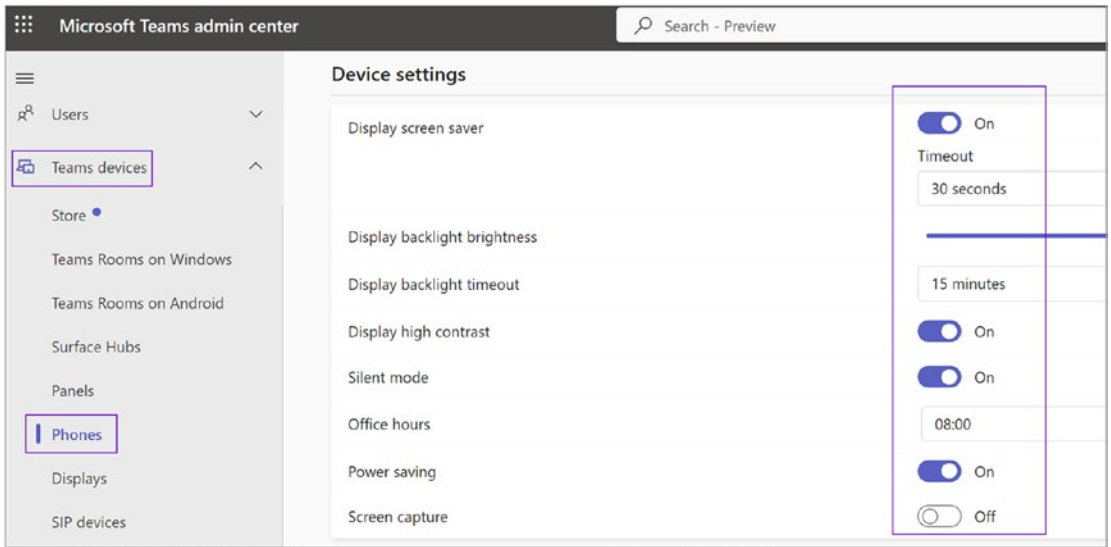


Figure 2-55. *Device config profile settings*

- d. Under Network Settings, select if you will enable DHCP or logging and if you will configure Host Name, Domain Name, IP Address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS, Device's Default Admin Password, and Network PC Port. Figure 2-56 shows a sample profile configuration with network settings.

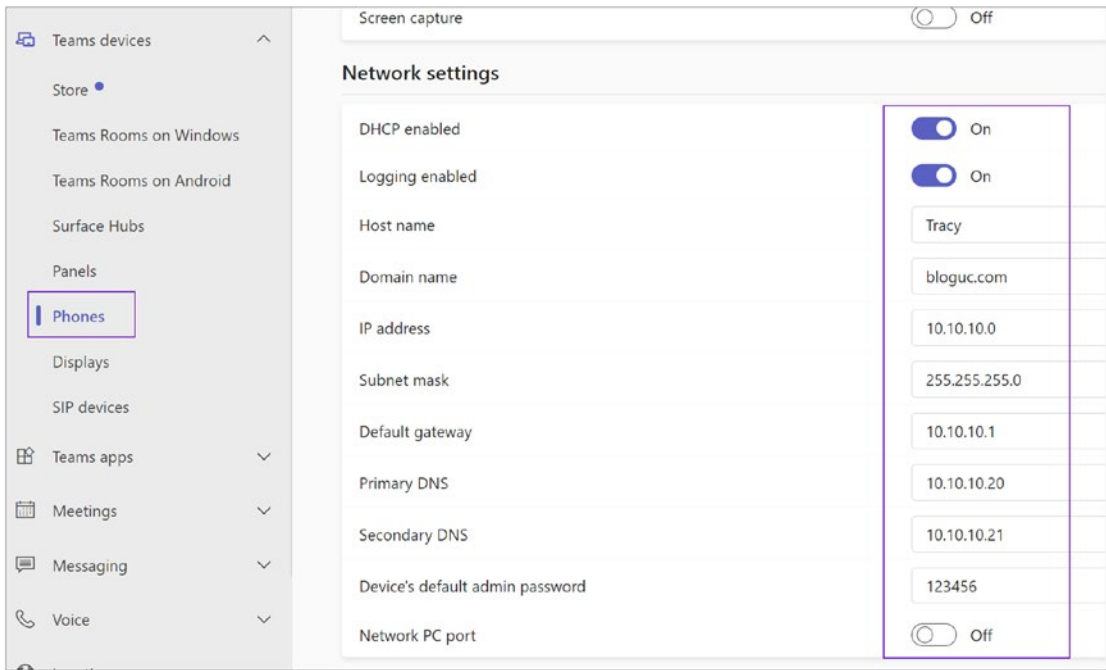


Figure 2-56. Configuration profile network settings

4. Once you complete the configuration profile settings, click Save to commit the profile configuration. The next step is to assign the configuration to a device or group of devices.

Assigning the Configuration Profile to Devices

After creating the configuration profile, you need to assign it to the appropriate devices.

To assign a configuration profile, follow these steps:

1. In the Microsoft Teams admin center, on the Phones page, select Configuration Profiles.
2. Select the policy (just select the check mark) you want to apply (e.g., Bloguc VVX & Trion Phone in Figure 2-57), and then click Assign To Device.
3. On the “Assign devices to a configuration profile” page, select the appropriate devices and then click Apply. Figure 2-57 shows assignment of the configuration profile to a phone device.

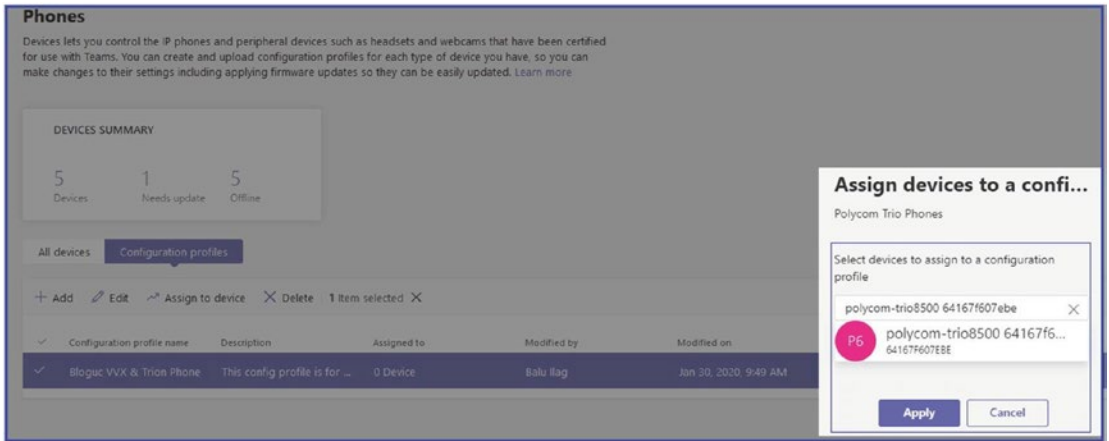


Figure 2-57. Assigning a configuration profile to a device

After a configuration profile is assigned, the settings of this profile will be applied to the selected devices.

Managing for Phone Inventory

You can manage phone inventory, including viewing and managing all phones. This includes admin tasks such as updating phones, restarting phones for maintenance, and monitoring and diagnostics. You can also create and assign configuration profiles. Figure 2-58 shows the available management options.

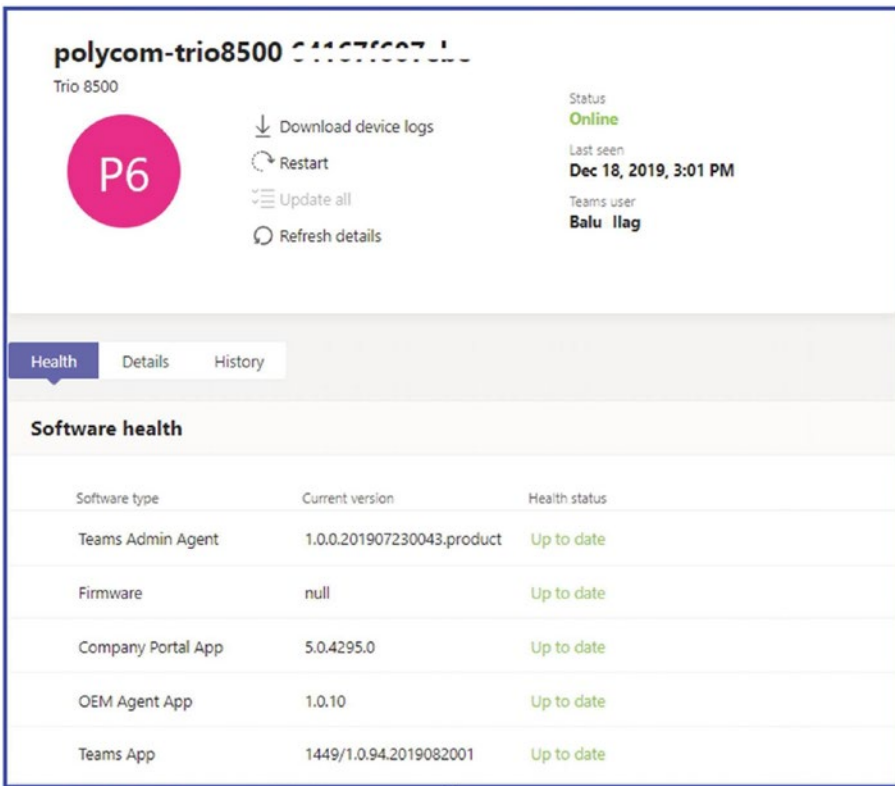


Figure 2-58. Phone management options

Configuring and Managing Microsoft Teams Rooms

Let’s look at configuring and managing rooms.

Managing Microsoft Teams Rooms

Microsoft Teams Rooms (MTR), previously known as Skype Room Systems, offers a complete meeting experience, bringing HD video, audio, and content sharing to meetings of all sizes, from small huddle areas to large conference rooms. Before configuring an MTR resource account, an admin must understand the environments, room size, layout, and purpose. You can then identify the capabilities you want each room to have in the future. When you create an inventory of the equipment and capabilities in each existing room, your requirements for that room feed into your device selection planning to create a rich conferencing solution. The audio and video capabilities that are needed for each room, as well as the room size and purpose, all

play an important role in deciding which solution will be optimal for each room. You must also check and confirm that the room doesn't have excessive echo, noisy air conditioning, or furniture getting in the way of the equipment. You should also confirm there is enough power for the screens and rooms.

As an MTR admin, your role is critical in ensuring that your organization gets the maximum benefit from its MTR system, providing an excellent meeting experience for all users. Remember, though, that each organization's specific needs and requirements may necessitate additional responsibilities. Always ensure you're following your organization's guidelines and best practices. Please always review the Microsoft documentation for the most current and accurate information.

As an MTR admin, you will have various responsibilities to ensure a seamless meeting experience.

- **Configuration and setup:** Configure and set up MTR devices according to the room layout and user requirements. This includes setting up the AV devices and screens and ensuring the MTR console is correctly configured with the MTR app.
- **Software updates:** Regularly check for and apply software updates to the MTR devices. This is crucial for maintaining security and gaining new features or improvements.
- **Monitoring and troubleshooting:** Use the Teams admin center or other monitoring tools to regularly check the status and health of the MTR devices. Promptly troubleshoot and resolve any issues that arise.
- **User training:** Provide training and support to users on how to use the MTR system for their meetings.
- **Policies and access control:** Implement and enforce policies for room usage. Also, manage the room calendar settings in Microsoft 365 to control who can book the room.
- **Maintenance:** Regularly clean and maintain the physical equipment. Test the equipment regularly to ensure it's working correctly.

It is a best practice to make sure to have a plan for monitoring, administration, and management tasks on an ongoing basis. It is important to decide who will undertake these tasks early in your deployment. In planning for operations, factors you need

to consider are deciding who will manage team rooms and which help-desk queue will handle calls regarding them. As part of Teams room management, important administrative considerations include the following:

- As an admin, have a proper plan for managing and configuring the local accounts that are created by the MTR application installer.
- You can consider using Microsoft Azure Monitor to monitor the MTR deployment and report on availability, hardware and software errors, and the MTR application version. As of this writing, this monitoring facility is not available, but Microsoft plans to provide such monitoring in the future.
- An additional consideration is whether rooms will be domain-joined or a workgroup member. Domain-joined deployment includes multiple advantages, such as granting domain users and groups administrative rights and importing your organization's private root certificate chain automatically. We recommend joining your Teams room to the domain so that you don't have to manually install the root certificate.

After addressing these considerations, you can start preparing to host accounts for rooms. Remember, every MTR device requires a dedicated and unique resource account that must be enabled for both Microsoft Teams or Skype for Business Online and additionally for Exchange Online. This account must have a room mailbox hosted on Exchange Online and be enabled as a meeting room in the Teams or Skype for Business deployment. In Exchange, you need to configure calendar processing so that the device can automatically accept incoming meeting requests.

Note Meeting scheduling features will not work without a device account.

There are several best practices to adopt when managing MTR rooms. Create a resource account for a Teams room with a meaningful display name and description to easily locate the Microsoft Teams room. The display name is important because users will see it when searching for and adding MTR systems to their meetings. As an example, you could use the following convention: city initials, followed by room name and maximum capacity. The Lincoln room with an eight-person capacity in San Jose might have the display name SJ-LN-8.

Creating a Microsoft Teams Room Account

To create a new room mailbox, use the following Exchange Online PowerShell module:

```
New-Mailbox -Name "Bloguc Sunnyvale Room 1" -Alias Bl-SVL-6-01 -Room
-EnableRoomMailbox -Account $true -MicrosoftOnlineServicesID <Account>
-RoomMailboxPassword (ConvertTo-SecureString -String '*****'
-AsPlainText -Force)
```

Here's an example of configuring the settings on the room mailbox named Bloguc MTR Room1:

```
Set-CalendarProcessing -Identity "Bl-SVL-6-01" -AutomateProcessing
AutoAccept -AddOrganizerToSubject $false -DeleteComments $false
-DeleteSubject $false -RemovePrivateProperty $false -AddAdditionalResponse
$true -AdditionalResponse "This is a Microsoft Teams Meeting room!"
```

Once the Teams room account is ready, you can proceed to room device installation. Once your Teams Rooms system is physically deployed and the supported peripheral devices are connected, including screens, speakers, microphones, console panels, and so on, the next matter is providing the Teams account and the login to the Teams room using the resource account and password that you created earlier, in our example, Bl-svl-6-01@bloguc.com. You use a script to create a Teams account (see <https://docs.microsoft.com/en-us/microsoftteams/rooms/rooms-configure-accounts>).

To sign in, you first need to configure the Teams Rooms application to assign the Microsoft Teams Rooms resource account and password created earlier. That enables the Microsoft Teams Rooms system to sign into Microsoft Teams or Skype for Business and Exchange. It is important to leverage certified USB audio and video peripherals linked elsewhere in the document. Not doing so can result in unpredictable behavior. Additionally, the account also needs a rooms license or add-on license assigned.

As an admin, you can manually configure each Microsoft Teams Rooms system. Alternatively, you can use a centrally stored XML configuration file to manage the application settings and leverage a startup Group Policy object (GPO) script to reapply the configuration you want, each time the Microsoft Teams Rooms system boots. To leverage a centrally stored configuration, however, your room must be domain-joined.

After room deployment, you can run multiple tests to make sure everything works as per your expectations. Frequently check the call quality using the call quality dashboard.

Admin Center: Teams Apps Tab

The Teams Apps tab in the Microsoft Teams admin center provides a consolidated view of all the Teams apps within your organization. It allows Teams administrators to manage and control these apps effectively. Here's a rundown of the capabilities available in the Apps tab:

- **Manage apps:** Here, you can view all the apps available for your organization in Teams. This includes Microsoft's own apps, third-party apps, and custom apps built by your organization. For each app, you can see its name, publisher, status, and other details. Also, you can view, manage, and upload custom apps developed specifically for your organization.
- **Permission policies:** You can control what apps are available to which users. For instance, you can allow everyone in your organization to use a certain app, or you can restrict its use to certain departments or teams.
- **Setup policies:** These policies let you control which apps and shortcuts appear in the Teams app bar for your users. For example, you could add a shortcut to a frequently used app for a specific department.
- **Teams apps:** Monitor the usage of Teams apps in your organization.
- **App catalog:** View the catalog of apps that are available for your organization to install.
- **Manage app setup policies:** Configure and assign policies to set up teams with pre-installed apps that are pinned to the app bar in the Teams desktop and web clients.

Managing applications as an admin is not difficult; however, you must know how to set up and assign policies. The following sections contain detailed information about managing Teams apps.

Permission Policies

The Microsoft Teams admin center has app permission policy settings that control what apps are available to Teams users in your organization. You can use the Global (Org-wide) default policy and customize it, or you can create one or more policies to meet the needs of your organization. Basically, you can allow Microsoft apps, third-party apps, or tenant apps.

Using app permission policies, you can block or allow apps either organization-wide or for specific users. When you block an app, all interactions with that app are disabled, and it will no longer appear in Teams. For example, you can use app permission policies to disable an app that creates a permission or data loss risk to your organization, gradually roll out new third-party or custom-built apps to specific users, and simplify the user experience, especially when you start rolling out Teams across your organization.

Out of the box, you will see the Global (Org-wide default) policy, which is designed to allow all Microsoft apps, third-party apps, and tenant apps to all users in your organization. This policy is assigned and applicable to all users by default (unless a custom policy is assigned). Figure 2-59 shows the default policy.

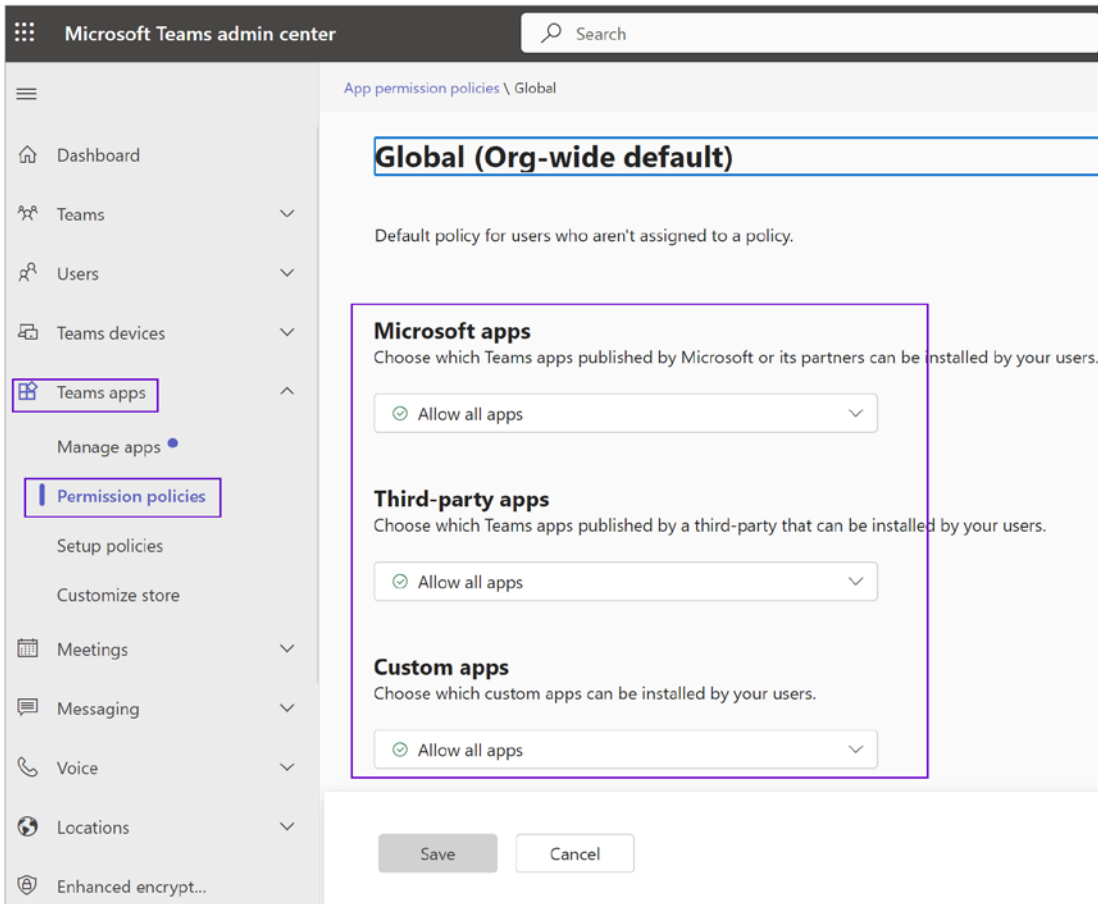


Figure 2-59. Teams global app permission policy

Managing Organization-wide App Settings

As a Teams admin, you can use organization-wide app settings to control which apps are available across your organization. Organization-wide app settings govern behavior for all users and override any other app permission policies assigned to users. You can use them to control malicious or problematic apps.

To manage org-wide app settings, log in to the Teams admin center and navigate to Teams Apps and select Manage Apps. Click Org-wide App Settings shown on the left side of the page. Once the Org-wide App Setting window opens, you can configure the settings you want to use. Figure 2-60 shows that tailored apps, third-party apps, and custom apps are allowed, and no apps are blocked. However, one setting that is not enabled is “Auto installed approved apps,” which is a newly added feature by Microsoft.

Org-wide app settings

Tailored apps

Users with F licenses will get tailored apps pinned on their behalf when they sign in to Teams. [Learn more](#)

Show tailored apps

On

Third-party apps

You can control which third-party apps can be installed for your organization. [Learn more](#)

Third-party apps ⓘ

On

New third-party apps published to the store ⓘ

On

Auto install approved apps ⓘ **New**

Off

When you use Auto install approved apps, you accept the terms of use, privacy policies, and permissions of each app.

[Manage selected apps](#)

Custom apps

You can develop and upload custom apps as app packages and make them available in your organization's app store. [Learn more](#)

Figure 2-60. App Org-wide settings

Why Is the Teams Apps Permission Policy Required?

Microsoft Teams app permission policies are necessary for various reasons. They allow administrators to have granular control over what applications can be accessed or installed by users in the organization; hence, they support both productivity and security.

Here's a deeper dive into why Teams app permission policies are essential:

- **Security:** These policies are essential to safeguarding your organization's data. By controlling which apps users can install and use, you prevent unauthorized or potentially malicious apps from gaining access to your company's data.
- **Compliance:** Certain industries have specific regulations regarding the types of software that can be used and the kind of data they can access. App permission policies can ensure your organization remains compliant with these regulations.
- **Productivity:** Not every app will be useful or necessary for every user. By customizing app permissions, you can streamline the Teams experience for your users, allowing them to focus on the tools that are most relevant to their work.
- **Control over third-party apps:** Some third-party apps might not be suitable for your business environment or might not meet your organization's standards for data privacy and security. With app permission policies, you can restrict these apps as needed.
- **User-specific needs:** Different teams within an organization may require different sets of apps. For example, the Marketing team might need social media management apps, whereas the Finance team might not. App permission policies allow customization according to the specific needs of different groups within the organization.

To sum it up, Teams app permission policies are a critical part of managing your organization's Teams environment, providing the flexibility to support a diverse set of user needs while maintaining data security and compliance.

Creating a Teams App Permission Policy

Admins create a custom app policy to control the apps that are available for different groups of users in an organization. You can create and assign separate custom policies based on whether apps are published by Microsoft or third parties or whether they are custom apps for your organization. It's important to know that after you create a custom policy, you can't change it if third-party apps are disabled in org-wide settings.

As an admin, you can be very specific about which applications you allow (Microsoft, third-party, or tenant apps) or block. You can allow all apps or just specific apps and block all apps such as Microsoft apps, third-party published apps, and tenant apps, or those published by your organization.

1. To create a custom app policy, log in to the Microsoft Teams admin center, and then navigate to Teams Apps. Select Permission Policies and then click +Add to create a new policy.
2. Once the app permission policy page opens, enter a name and description for the policy (e.g., **Bloguc App Policy1**).
3. The default setting for Microsoft apps is "Allow all apps."
4. Then, under Third-Party Apps, select "Allow specific apps and block all others," as shown in Figure 2-61. You then have to add the apps that you want to allow.

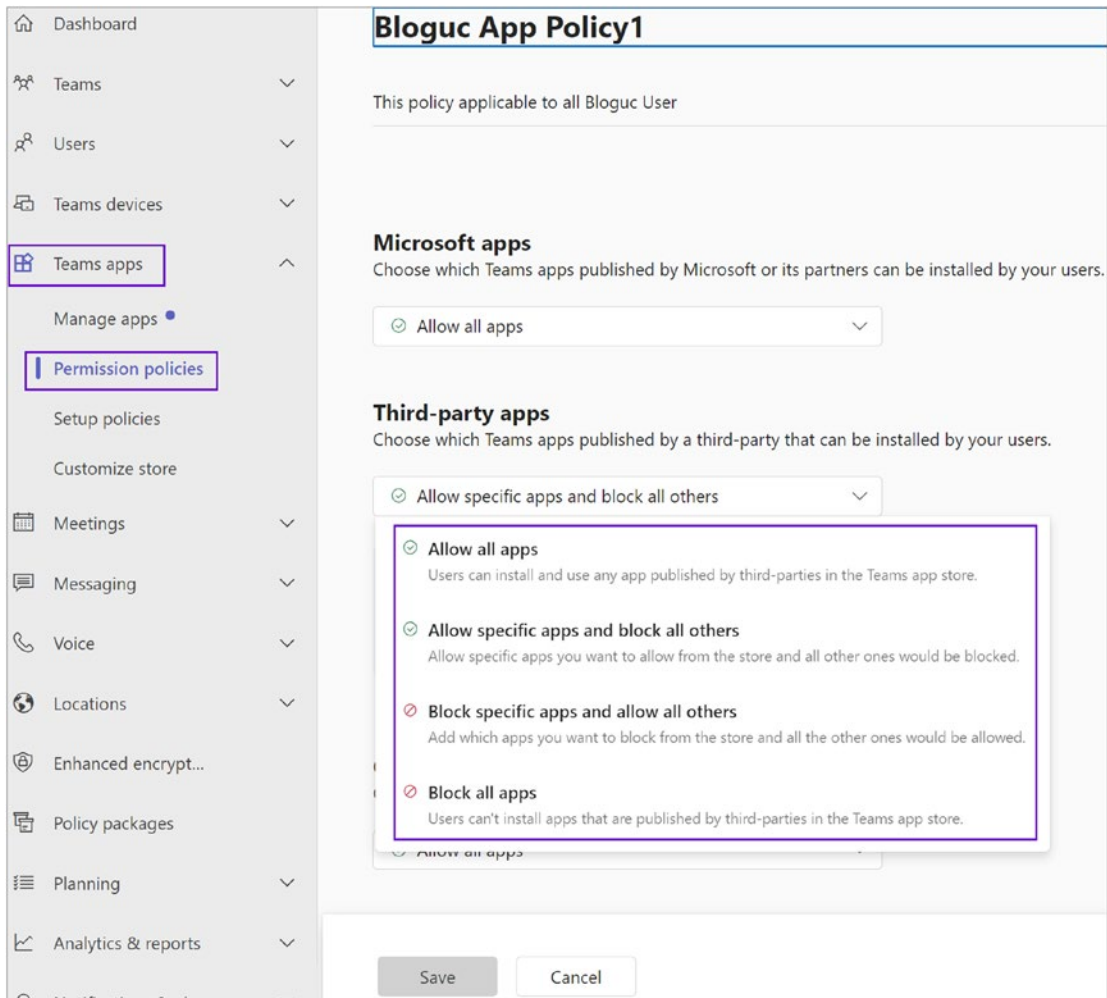


Figure 2-61. Allowing specific apps and blocking all others

5. Select “Allow apps” and then search for the app(s) that you want to allow. Make your selections and then click Add. The search results are filtered to the app publisher (Microsoft apps, third-party apps, or tenant apps). The example in Figure 2-62 shows that Workplace from Facebook is allowed.
6. Once you have chosen the list of apps, select Allow. Similarly, if you selected “Block specific apps and allow all others,” search for and add the apps that you want to block.

- Click Save to save the app policy. For the example shown in Figure 2-62, the Bloguc organization requirement is to allow all Microsoft apps and custom apps but block all third-party apps except Twitter apps.

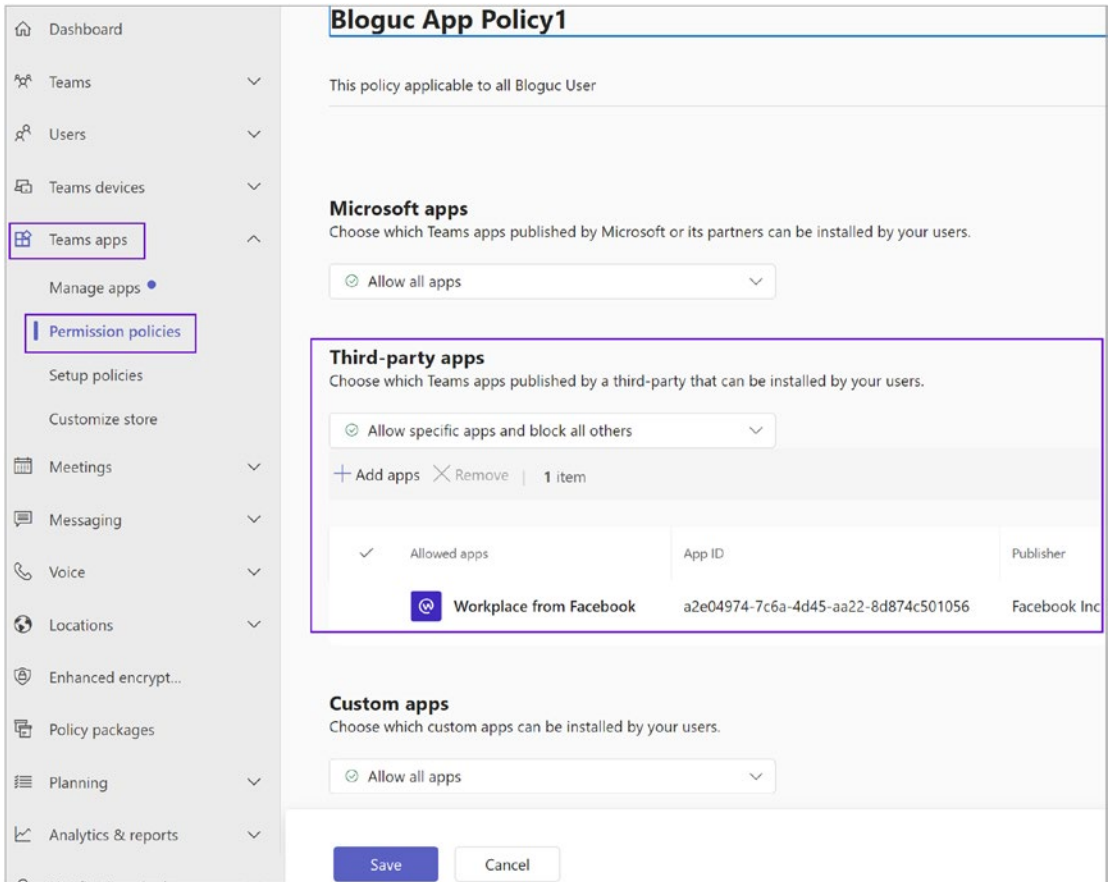


Figure 2-62. Teams app permission policy

Note All allowed apps will show in Teams client apps, and users can add to their teams and use them.

Assigning the App Permission Policy to Users

Once you create a custom policy, the next thing you need to do is to assign the policy to users so that the policy takes effect. As an admin, you can use the Microsoft Teams admin center to assign a custom policy to one or more users. Alternatively, you can use the Skype for Business PowerShell module to assign a custom policy to groups of users, such as all users in a security group or distribution group.

To assign a policy to users, follow this procedure:

1. Log in to the Teams admin center and then navigate to Teams Apps. Select Permission Policies.
2. Select the check box for the custom policy name and then click Manage Users.
3. In the Manage Users window, search for the user by display name or by username, select the name, and then select Add. Repeat this step for each user that you want to add, as shown in Figure 2-63.

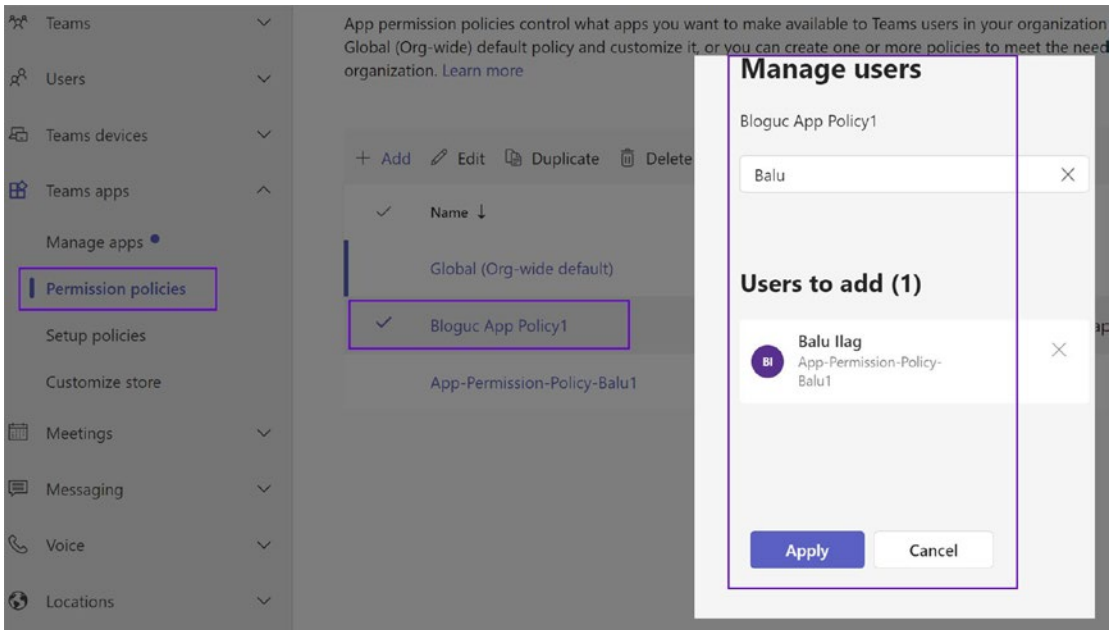


Figure 2-63. Assigning a policy to a user

4. Once you add the required users, click Apply to commit the change and assign the policy to those users.

You can assign custom app permissions to users on the Users tab in the Teams admin center. Simply log in to the Teams admin center, navigate to Users, and select the users. Click Edit Settings and then under App Permission Policy, select the app permission policy you want to assign; click Apply.

Assigning a Custom App Permission Policy Using PowerShell

As previously mentioned, you can assign a custom app permission policy to multiple users with PowerShell for automation. For example, you might want to assign a policy to all users in a security group. You can do this by connecting to the Azure AD PowerShell module and the Skype for Business Online PowerShell module and using the `Grant-CsTeamsAppPermissionPolicy` command.

For example, if you want to assign a custom app permission policy called Bloguc App Policy1 to all users in the Bloguc IT group, you would run the following command:

```
$group = Get-AzureADGroup -SearchString "Bloguc IT Group"
$members = Get-AzureADGroupMember -ObjectId $group.ObjectId -All $true |
Where-Object {$_.ObjectType -eq "User"}
$members | ForEach-Object { Grant-CsTeamsAppPermissionPolicy -PolicyName
"Bloguc App Policy1" -Identity $_.EmailAddress}
```

Depending on the number of members in the group, this command could take several minutes to execute.

Setup Policies

In Teams apps, the next type of policy is a setup policy. This is actually where you as an admin can control how apps will appear in the Teams client for users. You can use app setup policies to customize Microsoft Teams to highlight the apps that are most important for your users. You can select the apps to pin to the apps bar and the order in which they appear. App setup policies let you showcase apps that users in your organization need, including those built by third parties or by developers in your organization.

Figure 2-64 shows the default Teams app setup policy. You can see the app names such as Activity, Chat, Teams, Calendar, Calling, and Files. All these apps will be displayed in the Teams client in the same order as shown under “Setup policies.”

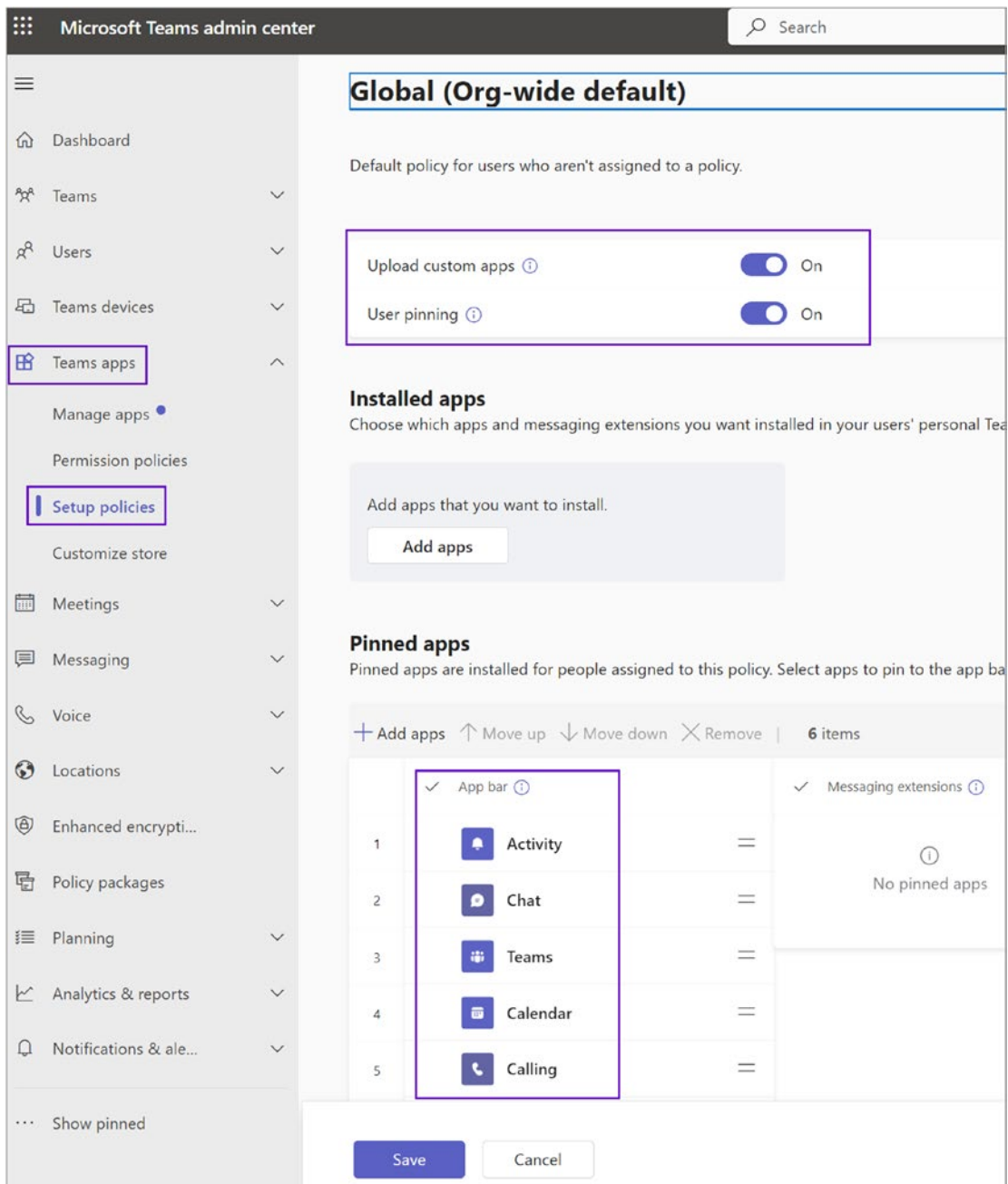


Figure 2-64. Setting setup policies

Figure 2-65 shows the result as it appears in the Teams client. The app bar displays on the side of the Teams desktop client and at the bottom for the Teams mobile clients.

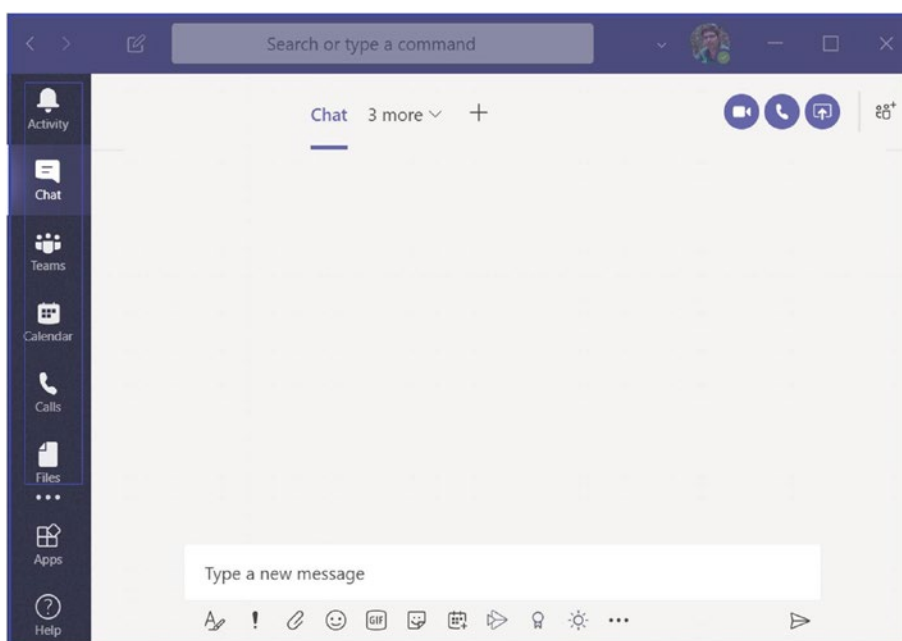


Figure 2-65. Teams apps set in a Teams setup policy

Managing the Teams Setup Policy

Microsoft Teams setup policies are rules that admins can configure to control what apps, bots, and other features should be pinned and visible in Microsoft Teams for end users. These policies help admins tailor the Teams experience to a user's role within the organization, making them more productive by having the necessary tools readily available.

In the Microsoft Teams admin center, setup policies can be found under Teams apps ► Setup policies. As part of managing Teams setup policies, you can create a custom app setup policy and add any Microsoft or custom apps as pinned apps. For example, the Bloguc organization wants to allow its users to see Planner as a pinned app in their Teams client. To add an app in a Teams app setup policy, follow these steps:

1. Log in to the Teams admin center, navigate to Teams Apps, and select Setup Policies. On the App Setup Policies page, select Add and then enter a name and description for the app setup policy.

2. Turn the Upload Custom Apps setting on or off, depending on whether you want to let users upload custom apps to Teams. You cannot change this setting if Allow Third-Party Or Custom Apps is turned off in the org-wide app settings in app permission policies. For this example, I have enabled Upload Custom Apps because the Bloguc organization wants users to allow custom apps.
3. In the Pinned Apps section, click Add Apps to search for the apps you want to add. When searching, you can optionally filter apps by app permission policy. Once you have selected your list of apps, click Add. In this example, we are adding Planner apps because the Bloguc organization wants to allow the Planner app, as shown in Figure 2-66.

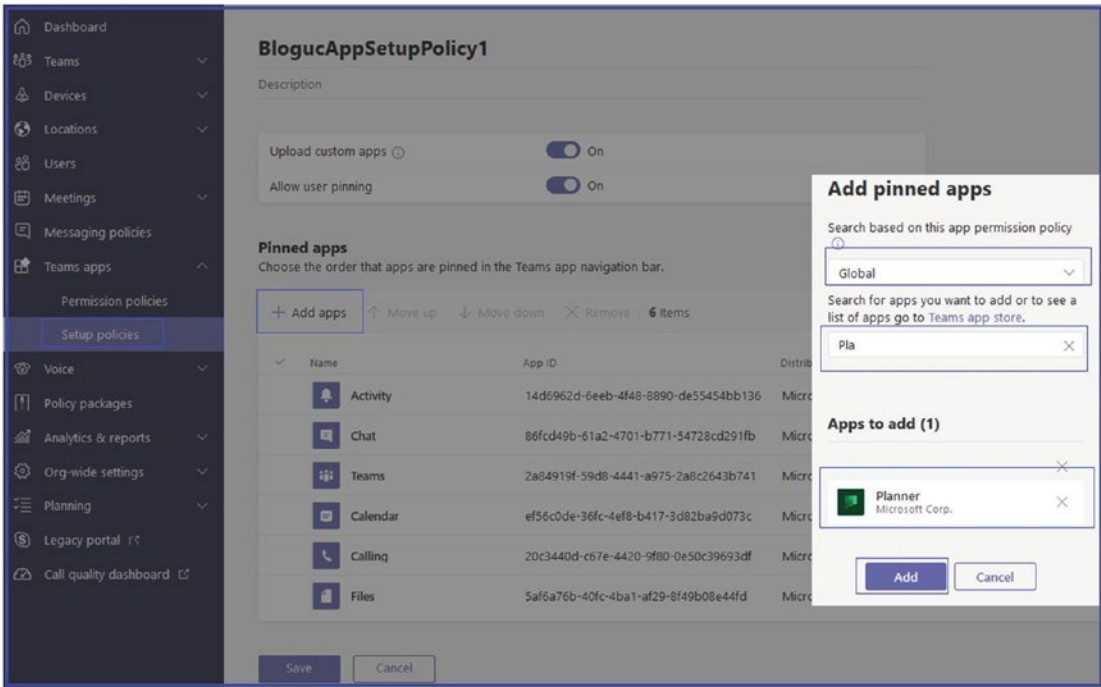


Figure 2-66. Adding apps to pinned apps

Once you click Add, the Planner apps will be included under “Pinned apps,” as shown in Figure 2-67.

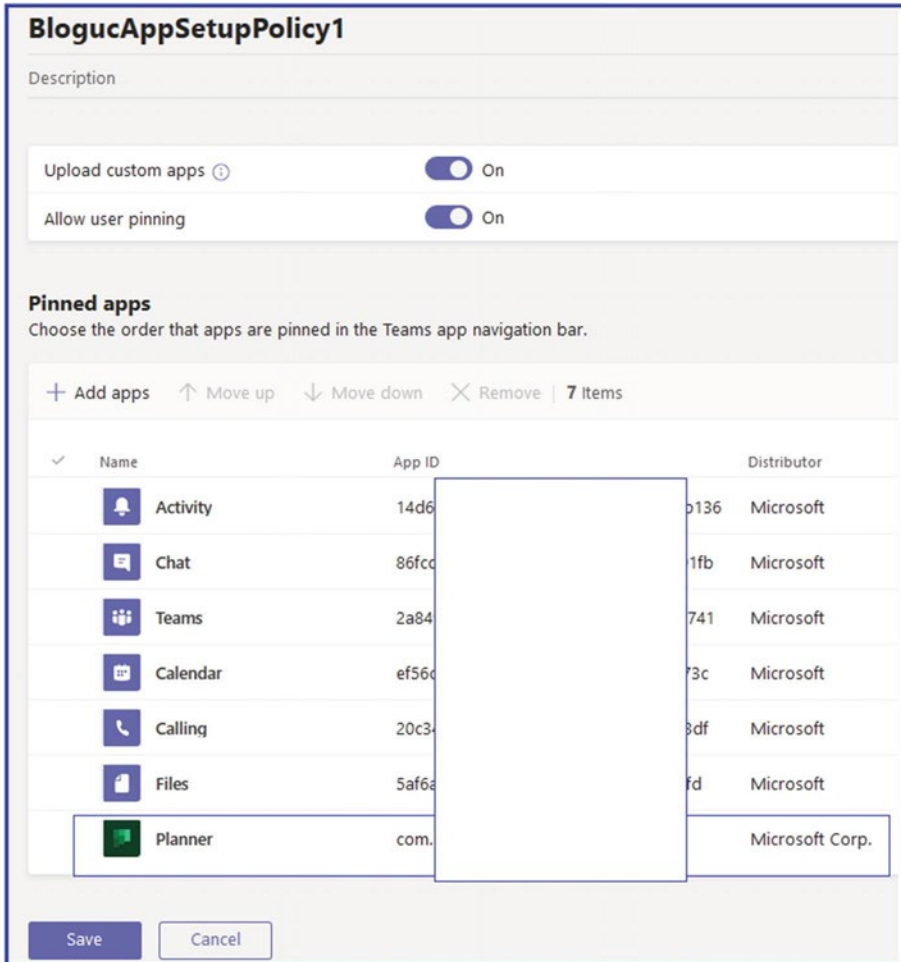


Figure 2-67. An app added to pinned apps

By leveraging setup policies, you can guide your team’s workflows and increase productivity by making the most commonly used apps readily accessible. You can have multiple policies for different teams based on their specific needs. It’s a powerful way to customize the Teams experience for your users.

Assigning a Custom App Setup Policy to Users from the Teams Admin Center and PowerShell

After creating a custom app setup policy, you need to assign the policy to users to show the custom apps added under pinned apps. There are multiple ways to assign an app setup policy to your users in the admin center. You can assign users either in setup policies or in Users in the Teams admin center or PowerShell.

To assign a policy using setup policies, follow this procedure:

1. Log in to the Teams admin center, and navigate to Teams Apps. Select Setup Policies and then select the policy by clicking to the left of the policy name. When you are done, click “Manage users.”
2. In the Manage Users window, search for the user by display name or by username, select the name you want, and then select Add. Repeat this step for each user you want to add, as shown in Figure 2-68. Click Apply.

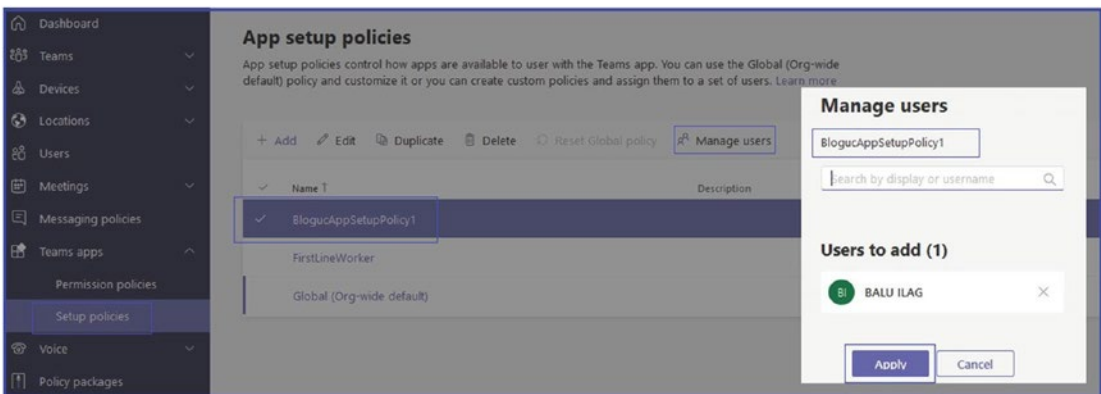


Figure 2-68. Assigning an app setup policy to a user

3. Once you are done adding users, click Save.

You can also perform the following steps if you want to assign users within the Users pane. Log in to the Teams admin center and then navigate to Users. Select the appropriate user and click Edit Settings. Under “App setup policy,” select the app setup policy you want to assign, and then click Apply.

Assigning a Custom App Setup Policy to Users Using PowerShell

As an admin, you might want to assign an app setup policy to multiple users that you have already identified. For example, you might want to assign a policy to all users in an IT group. You can do this by connecting to the Azure AD PowerShell for Graph module and the Skype for Business Online PowerShell module.

For example, to assign an app setup policy called `BlogucAppSetupPolicy1` to all users in the Bloguc IT group, you should execute the following PowerShell commands:

```
## Get the GroupObjectId of the particular group: ##
$group = Get-AzureADGroup -SearchString "***Bloguc IT**"
## Get the members of the specified group: ##
$members = Get-AzureADGroupMember -ObjectId $group.ObjectId -All $true |
Where-Object {$_.ObjectType -eq "User"}
## Assign all users in the group to a particular app setup policy: ##
$members | ForEach-Object { Grant-CsTeamsAppSetupPolicy -PolicyName
"**BlogucAppSetupPolicy1**" -Identity $_.EmailAddress}
```

Depending on the number of members in the Bloguc IT group, this command could take several minutes to execute.

These capabilities make it easier to manage the integration of apps into Teams, enhance security, and improve the Teams experience for your users. By having control over what apps are available and to whom, you can help ensure that your organization gets the maximum benefit from Teams while reducing the risks associated with unmanaged app usage. Always make sure to refer to the latest Microsoft documentation to get the most current and accurate information about managing apps in Teams.

Admin Center: Meetings Tab

The Meetings tab in the Microsoft Teams admin center is a centralized place for admins to manage and customize the meeting experiences for their organization. It offers a wide range of settings and configurations that can be tailored to suit the unique needs of your organization. You will find all the meeting and live event settings and policies under Meeting in the Teams admin center, as shown in Figure 2-69.

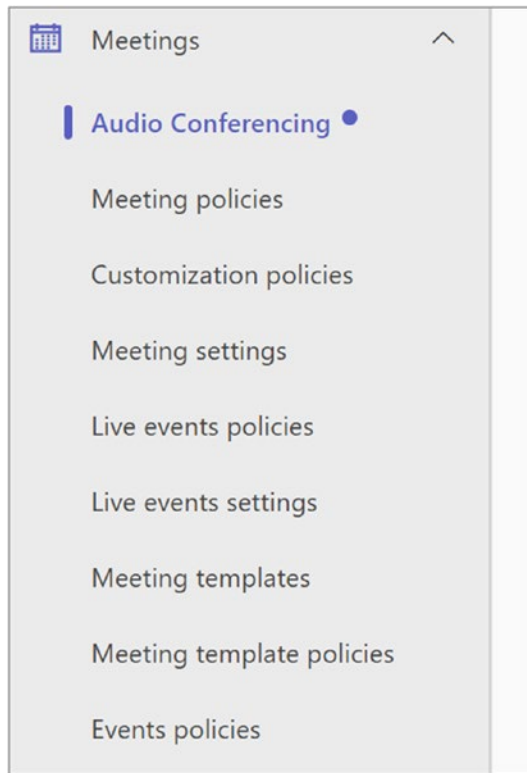


Figure 2-69. Meeting policy

Here’s what you can do on the Meetings tab:

Audio conferencing: The Audio Conferencing tab controls phone numbers and features available to users with audio conferencing. You can use the Global (Org-wide) default policy and customize it, or you can create one or more policies to meet the needs of your organization.

Meeting policies: Here, you can define what features are available to users during Teams meetings. You can control things such as screen sharing, recording permissions, video settings, and much more.

Customization policies: Use the customization policies tab to customize the look of your organization's Teams meetings. You can use the Global (Org-wide default) policy or create custom policies and assign them to a set of users. Remember this policy setting is available only with Teams Premium.

Meeting Settings: This is where global meeting settings are defined, including settings for third-party apps, cloud recording, transcription services, and the use of Microsoft Whiteboard.

Live Events Policies: This section allows you to define the settings for live events, including permissions and features for presenters and attendees.

Live Events Settings: Here you can manage global settings for live events, including permissions for third-party apps and default roles for attendees.

Meeting templates: Meeting templates can be used to create meetings that are available to users with common needs or a common project. Meeting templates are available to all organizations including small to large business and educational organizations. Remember this policy setting is available only with Teams premium.

Meeting templates policies: Meeting templates policies let you create and set up policies that control what templates people in your organization can see. You can use the Global (Org-wide default) policy and customize it, or you can create custom policies. Remember this policy setting is available only with Teams premium.

Event Policies: Teams Events Policies are used to configure event settings on Teams, starting with webinars. You can use the Global (Org wide default) policy and customize it, or you can create custom policies and assign them to people who create, run, and manage events in your organization.

Why Is Teams Meeting So Important?

Meetings play a crucial role in today's business environment, especially with remote work becoming increasingly prevalent. Effective meetings can help in the following ways:

Improve communication: They provide a platform for open discussion and immediate feedback. This helps to ensure that everyone is on the same page and any misunderstandings can be cleared up promptly.

Facilitate collaboration: Meetings bring people together to work toward common goals. They encourage teamwork and foster a culture of collaboration.

Drive decision-making: They offer an opportunity for decision-makers to come together to discuss, debate, and make important decisions.

Boost productivity: Regular meetings keep everyone updated about the ongoing projects, work progress, and next steps, which helps in maintaining momentum and productivity.

Detailed Information for All the Meeting Policies

Microsoft Teams meetings are one of the most used and best features Teams provides. We already covered the basic details of Teams meetings in Chapter 1. If you are new to Teams meeting, we encourage you to review Chapter 1. Once you are aware of how to set up teams, channels, and applications within Microsoft Teams, the next step you can take is to add and customize settings and policies for meetings, including audio conferencing, video, and application sharing.

Users can schedule and join Teams meetings from a variety of clients. For example, using audio conferencing, users can attend meetings from land lines or mobile phones by dialing in to the meeting. As a Teams admin, you can enable or disable certain types of meetings in addition to disabling modalities such as video or screen sharing, according to organization regulations. Because there is integration between Teams and Office 365 tools such as Microsoft Outlook, you can use an add-in to schedule Teams meetings directly from your calendar. Based on your organization's needs and requirements, you can configure the appropriate settings for meetings and conferencing

that your employees are going to use in Microsoft Teams. Because Teams offers so many options and advantages, it is important for you as an admin to review and confirm that your environment is properly configured to provide your users with the best possible experience.

Audio Conferencing

Audio conferencing policies allows admins to manage phone numbers and features available to users with audio conferencing. You can use the Global (Org-wide) default policy and customize it, or you can create one or more policies to meet the needs of your organization. Figure 2-70 shows an audio conferencing policy example.

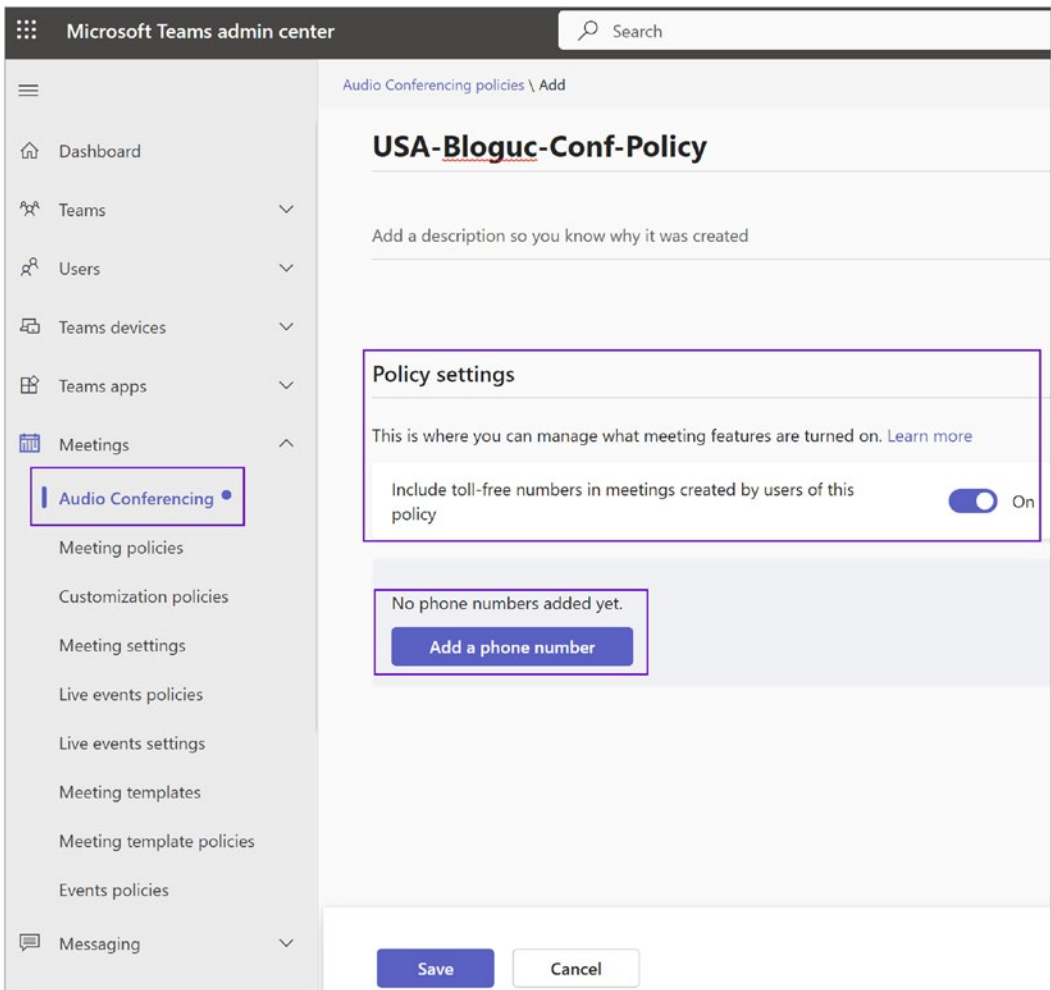


Figure 2-70. Meeting audio conferencing

Meeting Policies

Meeting policies are used to control what features are available to users when they join Microsoft Teams meetings. You can use the Global (Org-wide default) policy and customize it or create one or more custom meeting policies for people who host meetings in your organization. Along with meeting policies, you can permit or restrict the features that will be available to users during meetings and audio conferencing. You must first decide if you are going to customize the initial meeting policies and whether you need multiple meeting policies. Then you must determine which groups of users receive which meeting policies. By default, there are six policies available including Global (Org-wide default), AllOn, AllOff, Restricted Anonymous access, Restricted Anonymous No Recording, and Kiosk.

Creating a New Meeting Policy or Customizing an Existing Policy

As a Teams admin, you must create or customize default Teams meeting policies as per your organization's requirements. Meeting features are controlled by creating and managing meeting policies, which are then assigned to users. You can manage meeting policies within the Microsoft Teams admin center or by using Windows PowerShell. Applied policies will directly affect the users' meeting experience before the start of the meeting, during the meeting, and after the meeting ends. Meeting policies can be applied in three different ways:

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

Remember that a 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. As a Teams admin, you can decide if changes must be made to this policy, or you can choose to create one or more custom policies and assign those to users.

Creating a New Meeting Policy

In a meeting policy there are six sections: Meeting scheduling, Meeting join & lobby, Meeting engagement, Content sharing, Recording & transcription, Audio & Video, and Watermark. To create a new meeting policy, follow these steps:

1. First, log in to the Teams admin center. From the left-hand navigation menu, select Meetings, and then click 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. For example, I gave the policy name **USA-Bloguc-Meeting-Policy**.
 - **Private meeting scheduling:** By default, this setting is on. When this setting is On, meeting organizers allow users to schedule private meetings.
 - **Meet now in private meetings:** By default, this setting is on. This option controls whether a user can start an instant private meeting.
 - **Channel meeting scheduling:** By default, this setting is on. When this setting is On, meeting organizers allow users to schedule channel meetings within channels that the users belong to.
 - **Meet now in channel meetings:** By default, this setting is on. When this setting is On, meeting organizers allow users to start instant meetings within channels that the users belong to.
 - **Outlook Add-In:** By default, this setting is on. When this setting is On, meeting organizers allow users to schedule private meetings from Outlook. This option is important because users can schedule Teams meetings through Outlook using add-in.
 - **Meeting registration:** By default, this setting is on. When this setting is On, meeting organizers can require registration to join a meeting.

- **Who can register:** By default, this setting is Everyone. This setting determines who can register for meetings (if Meeting registration is On): Everyone or People in my organization.
- **Attendance report:** By default, this setting is Everyone, unless organizers opt out. This setting gives meeting organizers the ability to see the toggle that turns on or off attendance reports within the Meeting options.
- **Who is in the report:** By default, this setting is Everyone, but participants can opt out. This setting controls whether participants in the meeting can opt in or out of offering their attendance information in the attendance report.
- **Attendance summary:** By default, this setting is “Show everything.” This setting controls whether to show attendance time information, such as join times, leave times, and in-meeting duration, for each meeting participant.

Figure 2-71 shows all of those options turned on in the “Meeting scheduling” section.

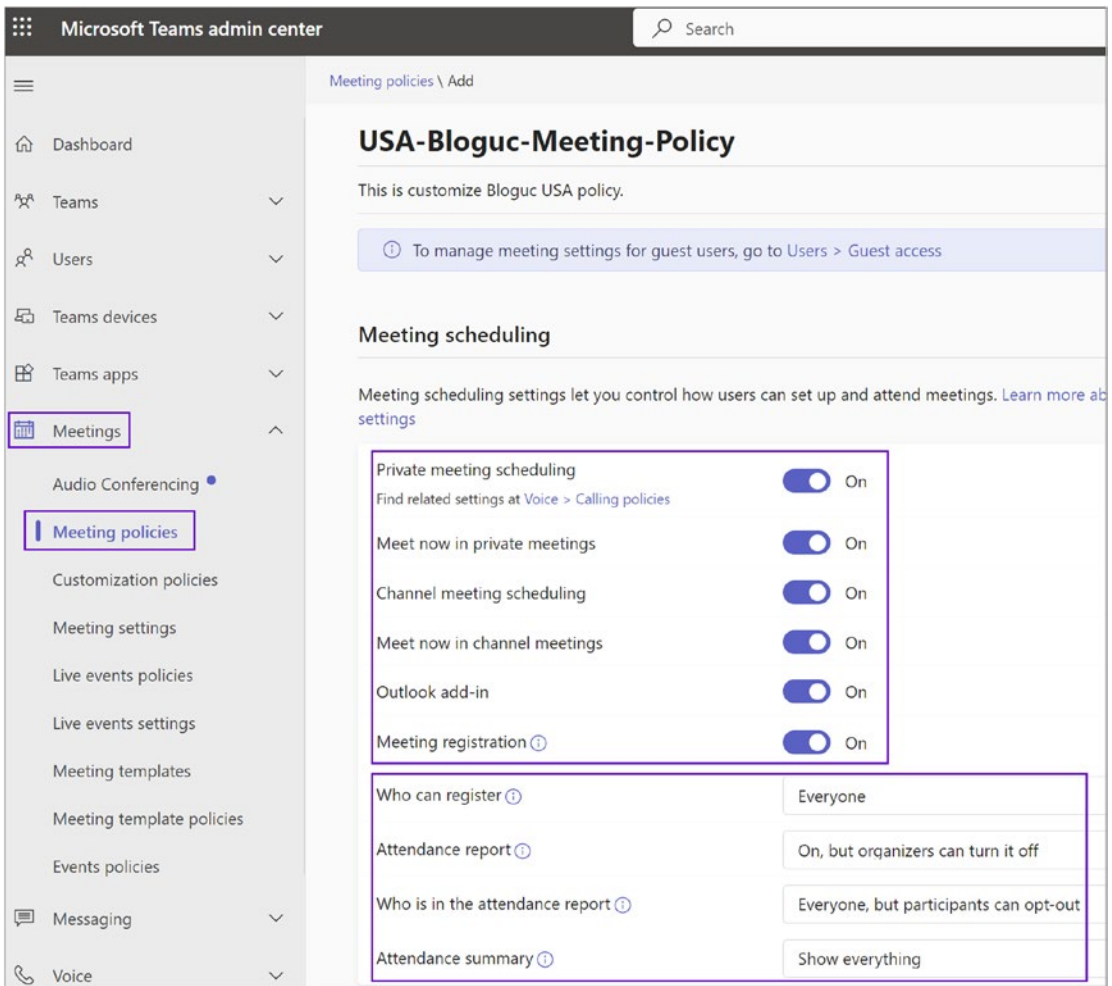


Figure 2-71. Meeting policies, scheduling option

For example, Meet Now in channel meetings is a policy setting that is applied before starting the meetings, and it 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 setting 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.

The next policy setting options are “Meeting join and lobby” and “Meeting engagement.” The “Meeting join and lobby” settings let you control how people join meetings and allow you to manage the lobby for Teams meetings. The “Meeting engagement” policy settings let you control how people interact in meetings. Figure 2-72 shows all of those options turned on in the “Meeting scheduling” section.

- **Anonymous users can join a meeting:** By default, this setting is on. When this setting is On, anyone can join Teams meetings, including Teams users in other organizations who aren't on your allowed domains list. If anonymous join is turned off in org-wide meeting settings, anonymous users can't join any meetings, regardless of what you set here.
- **Anonymous users and dial-in callers can start a meeting:** By default, this setting is off. When this setting is turned on, anonymous users and dial-in callers can start a meeting without someone in attendance. When this setting is off, they must wait in the lobby until the meeting is started by someone in your organization, a guest, or a user from a trusted organization. This setting works only if "Anonymous users can join a meeting" is turned on both in the org-wide meeting settings and in this meeting policy and "Who can bypass the lobby" is set to Everyone.
- **Who can bypass the lobby:** By default, this setting is "People in my organization and guests." This setting can control who can join a meeting directly and who must wait in the lobby until they're 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:** By default, this setting is off. This setting 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. When this setting is turned off, dial-in callers must wait in the lobby until they're admitted. This setting controls the default value for Meeting options; organizers and co-organizers can change this when they set up Teams meetings.
- **Meeting chat:** By default, this setting is on for everyone. This setting controls which meeting attendees can participate in the meeting chat. When turned off for anonymous participants, they can read the chat but not post messages.
- **Q&A:** By default, this setting is on. When this setting is On, organizers can enable a question and answer experience for their meetings.

- **Reactions:** By default, this setting is on. This setting controls whether users can use live reactions such as Like, Love, Applause, Laugh, and Surprise in Teams meetings.

Figure 2-72 shows all of those options for meeting join and lobby and meeting engagement section.

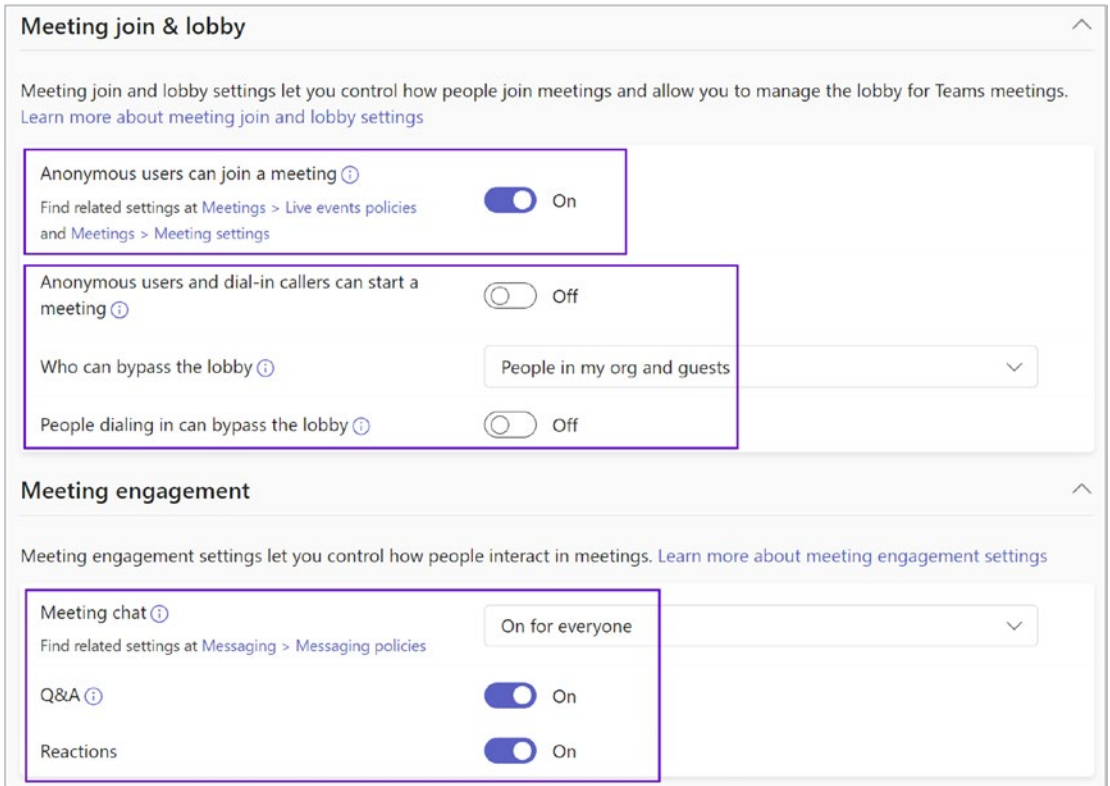


Figure 2-72. Meeting policies: meeting join and engagement option

- The next policy setting option is “Content sharing settings,” which allows you to control the different types of content that can be used during Teams meetings that are held in your organization.
 - Who can present:** By default this setting is Everyone. You can control who can be a presenter in Teams meetings. Organizers and co-organizers can change this when they set up Teams meetings.

- b. **Screen sharing mode:** By default this setting is set to “Entire screen.” You can control whether desktop and window sharing is allowed in the user’s meeting.
- c. **Participants can give or request control:** By default, this setting is on. You can control whether the user can give control of the shared desktop or window to other meeting participants. This setting isn’t supported if either user is using in Teams in a browser.
- d. **External participants can give or request control:** By default, this setting is off. This setting controls whether external participants, anonymous users, and guests can be given control or request control of people in your organization’s shared screen during a Teams meeting. This setting must be turned on in both organizations for an external participant to take control.
- e. **PowerPoint Live:** By default, this setting is on. You can control whether a user can share PowerPoint slide decks in a meeting. External participants, including anonymous, guest, and external access users, inherit the policy of the meeting organizer.
- f. **Whiteboard:** By default this setting is on. You can control whether a user can share the whiteboard in a meeting. External participants, including anonymous, guest, and external access users, inherit the policy of the meeting organizer.
- g. **Shared notes:** By default this setting is on. When this setting is on, attendees can create shared meeting notes through the meeting details.

Figure 2-73 shows the content sharing settings and the ways the settings can change based your organization needs.

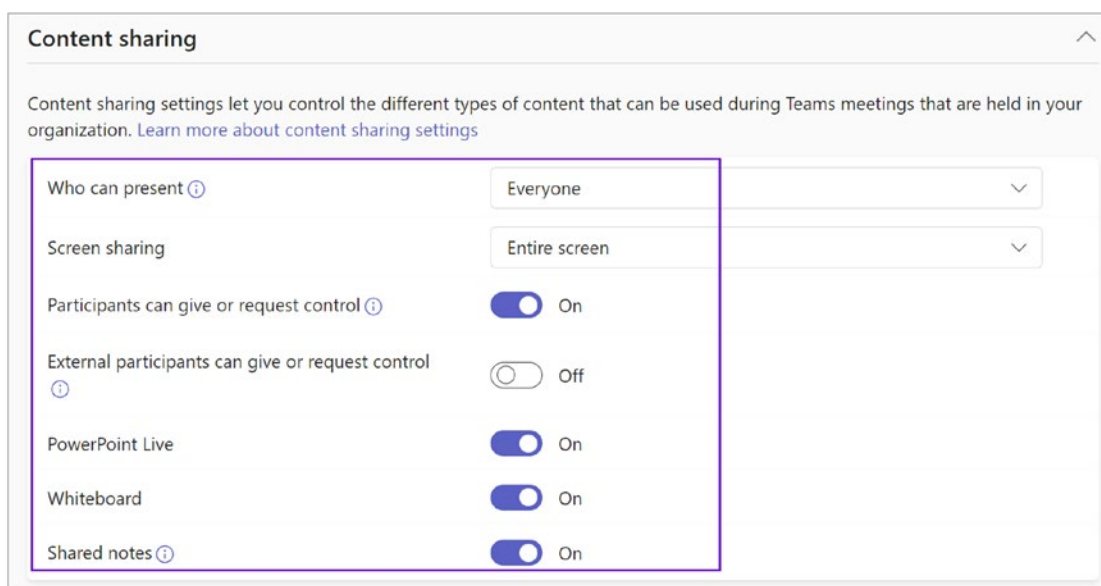


Figure 2-73. Meeting policies: Content sharing

- The next setting is “Recording and transcription.” Recording and transcription settings let you control how these features are used in a Teams meeting. As part of recording and transcription, you can customize the following setting options. Figure 2-74 shows the recording and transcription settings:
 - **Meeting recording:** By default this setting is on. When this setting is on, users can record their Teams meetings and group calls to capture audio, video, and screen sharing activity. The meeting organizer and recording initiator need to have recording permissions to record the meeting.
 - **Recordings automatically expire:** By default this setting is on. When this setting is on, meeting recordings automatically expire in the number of days shown in the “Default expiration time” setting.
 - **Default expiration time:** By default, expiration set as 120 days. The default expiration time for new meeting recordings is from 1 to 99999 days. Recordings that automatically expire must also be turned On.

- **Store recordings outside your country or region:** By default this setting is off. If you want to store meeting recordings outside of your country or region, turn on this setting. This setting isn't applicable to recordings stored in OneDrive or SharePoint.
- **Transcription:** By default this setting is on. You can control whether captions and transcription features are available during playback of meeting recordings. The person who started the recording needs this setting turned on for these features to work with their recording.
- **Live captions:** By default this setting is off, but organizers and co-organizers can turn them on. This setting is a per-user policy and applies during a meeting. This setting controls whether the “Turn on live captions” option is available for the user to turn on and turn off live captions in meetings that the user attends.

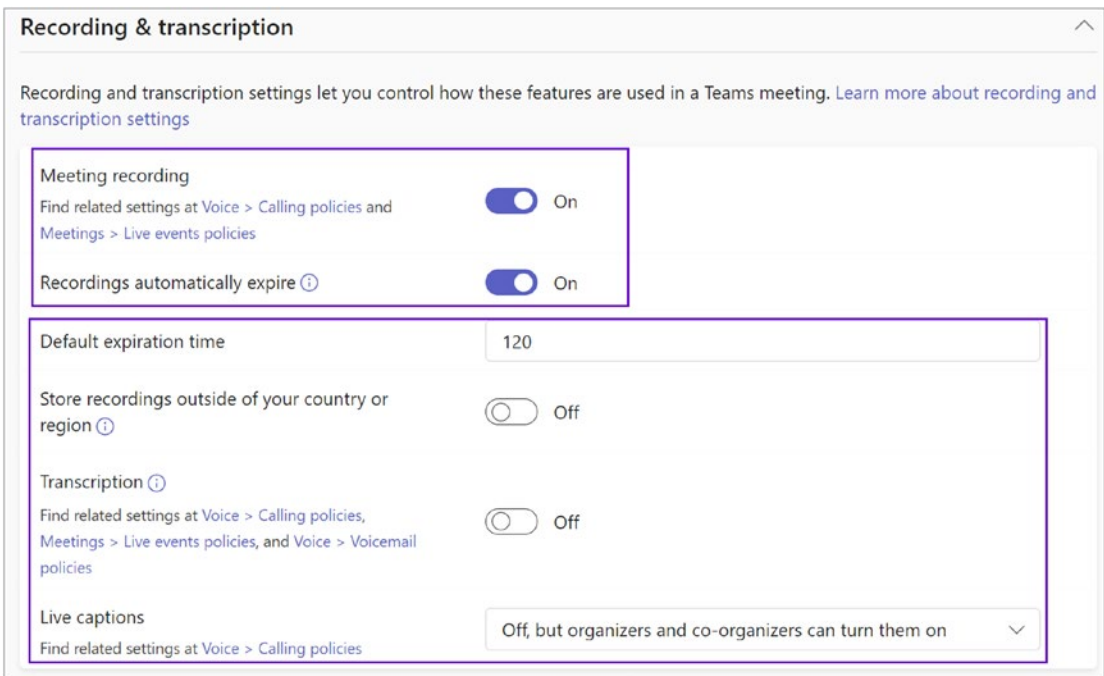


Figure 2-74. Meeting policies: Recording and transcription

- The next and last settings are in the “Audio & Video and watermark” section. Audio and video settings allow you turn on or off features that are used during Teams meetings. An additional setting is to add a watermark to content and videos shared in Teams meetings to protect confidential data.
 - **Mode for IP audio:** By default this setting is set to **Outgoing**, and incoming audio is enabled. This setting controls whether incoming and outgoing audio can be turned on in meetings and group calls.
 - **Mode for IP video:** By default this setting is set to **Outgoing**, and incoming audio is enabled. This setting controls whether incoming and outgoing video can be turned on in meetings and group calls.
 - **IP Video:** By default this setting is on. This setting controls whether video can be turned on in meetings hosted by a user and in one-on-one and group calls started by a user. On Teams mobile clients, this setting controls whether users can share photos and videos in a meeting.
 - **Local broadcasting:** By default this setting is off. Use NDI or SDI technology to capture and deliver broadcast-quality audio and video over your network.
 - **Media bit rate (Kbs):** By default, this value is set as 50000. This setting determines the media bit rate for audio, video, and video-based app sharing transmissions in calls and meetings for the user. It’s applied to both the uplink and downlink media traversal for users in the call or meeting. This setting gives you granular control over managing bandwidth in your organization.
 - **Network configuration lookup:** By default this setting is off. When it is on, roaming policies in network topology are checked.
 - **Participants can use video effects:** By default this setting is set to all video effects. You can control if participants can customize their camera feed with video background images and filters.

- **Live streaming:** By default this setting set as off. This determines whether you provide support for your users to stream their Teams meetings to large audiences through the Real-Time Messaging Protocol (RTMP).
- **Watermark videos:** By default this setting is off. This setting controls watermarks on attendee videos.
- **Watermark shared content:** By default this setting set as off. This setting controls watermarks on content shared on the screen in a meeting.

Figure 2-75 shows the “Audio & video” meeting settings and Watermark setting.

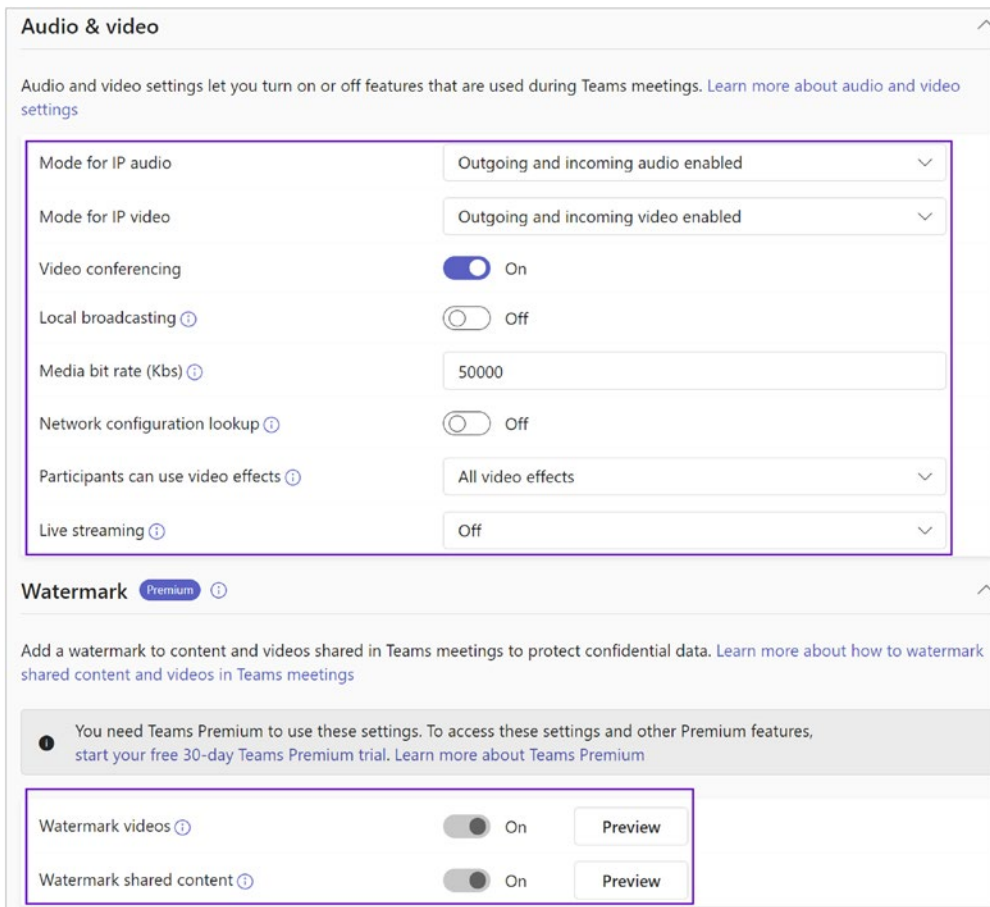


Figure 2-75. “Audio & video” settings and Watermark setting options

Meeting Policy Assignment

Once you create a meeting policy, the next thing you have to do is to assign the policy to a user or group of users for it to take effect. There are two ways to assign a policy to a user using the Teams admin center in both the Users and Meeting Policies sections.

- To assign a policy using the Meeting Policies tab, simply log in to the Teams admin center, navigate to Meetings, and select Meeting Policies. Select the required meeting policy and then click Manage Users. In the “Manage users” drop-down window, select “Assign users” and start entering a username. Once the full username shows, click Add and then click Apply to apply the policy. Figure 2-76 shows user Balu Ilag added to the applied policy.

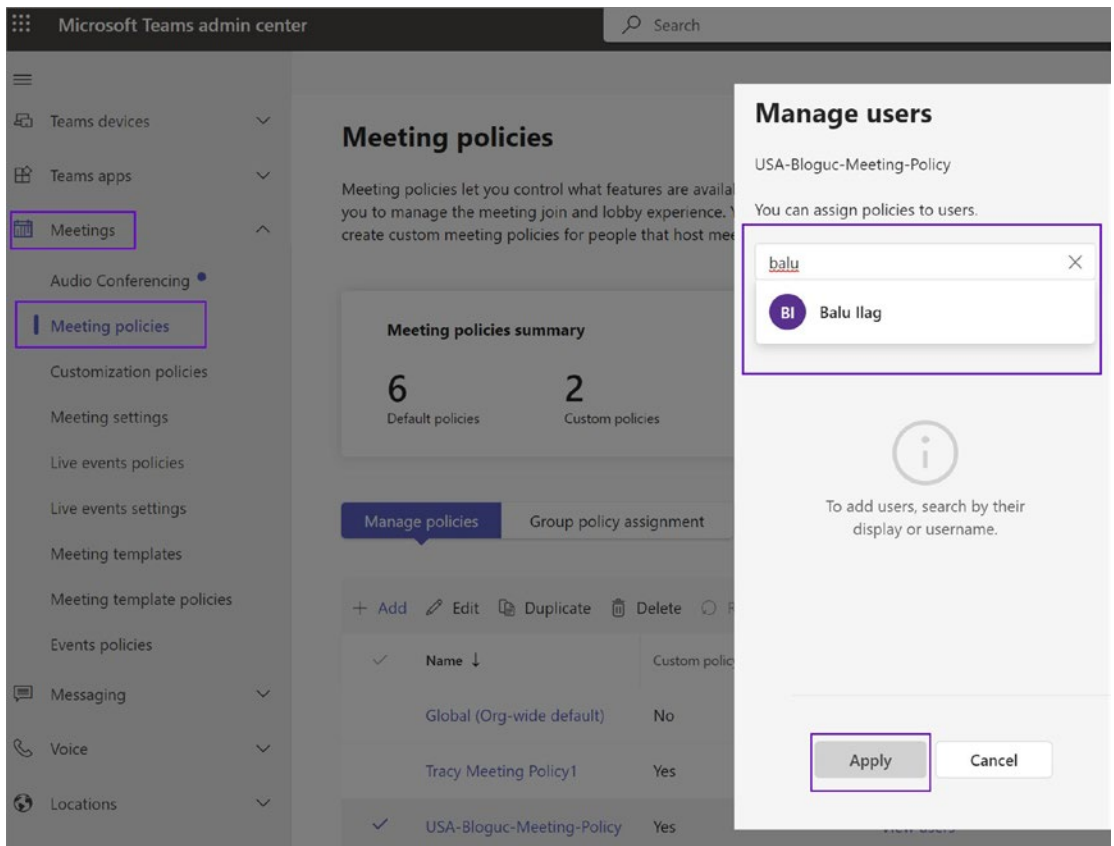


Figure 2-76. Policy assigned to user

- To assign a policy using the Users section in the Teams admin center, log in to the Teams admin center, and then navigate to Users. Select the users to whom you want to apply the policy and then click the Policies section. Under Edit User Policies, select the appropriate meeting policy, and then click Apply, as shown in Figure 2-77.

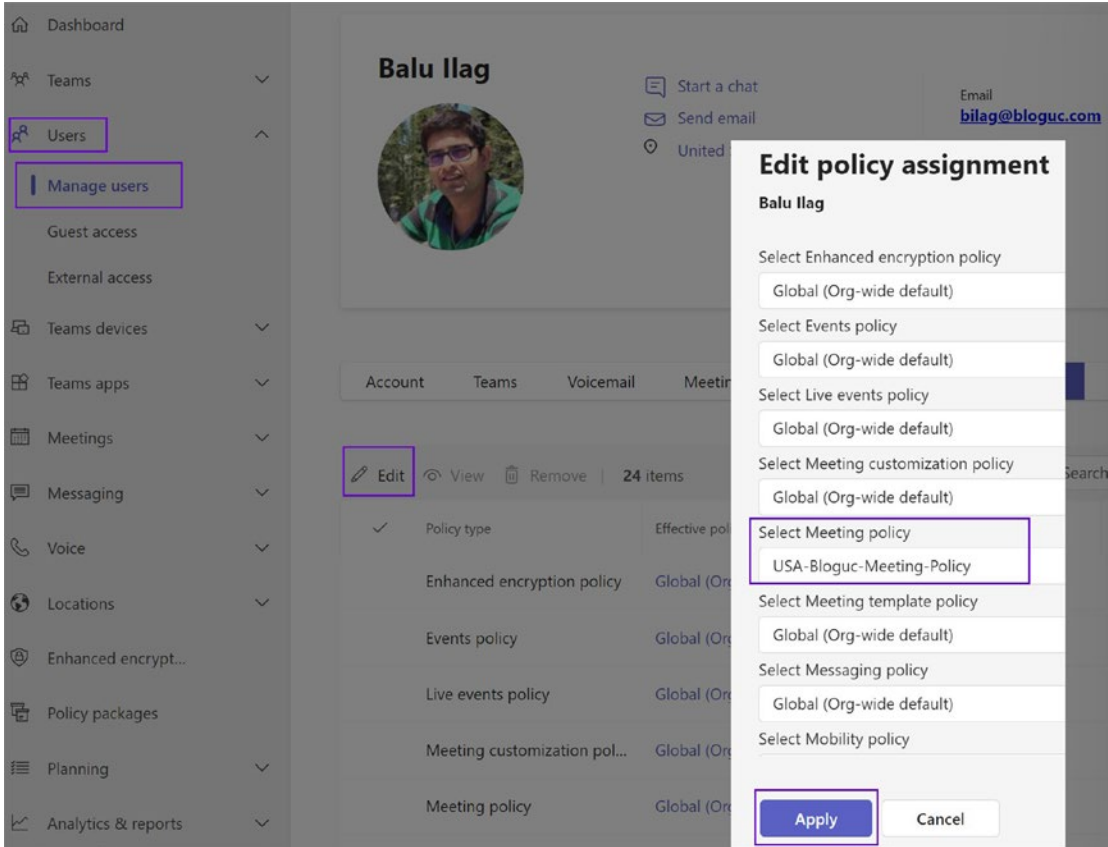


Figure 2-77. Assigning policies from the Users tab

As previously mentioned, you can also create a meeting policy using PowerShell. To do so, you must use the `New-CsTeamsMeetingPolicy` cmdlet. Once the policy is ready and you can modify settings, then use the command `Set-CsTeamsMeetingPolicy`.

In this example, we create a new meeting policy with the identity BlogucMeetingPolicy1. In this example, two different property values are configured: AutoAdmittedUsers is set to Everyone, and AllowMeetNow is set to False. All other policy properties will use the default values.

```
New-CsTeamsMeetingPolicy -Identity BlogucMeetingPolicy1 -AutoAdmittedUsers "Everyone" -AllowMeetNow $False
```

As an example, consider the setting titled AllowTranscription. This setting controls whether meetings can include real-time or post-meeting captions and transcriptions. If you want to enable this setting on an existing meeting policy titled BlogucMeetingPolicy1, you should run the following command:

```
Set-CsTeamsMeetingPolicy -Identity BlogucMeetingPolicy1 -AllowTranscription $True
```

Customization Policies

Customize your meetings with your organization's logo, colors, or other visuals. Customization policies are available for meeting organizers with a Teams Premium or Advanced Communications license. Figure 2-78 shows the customization policies.

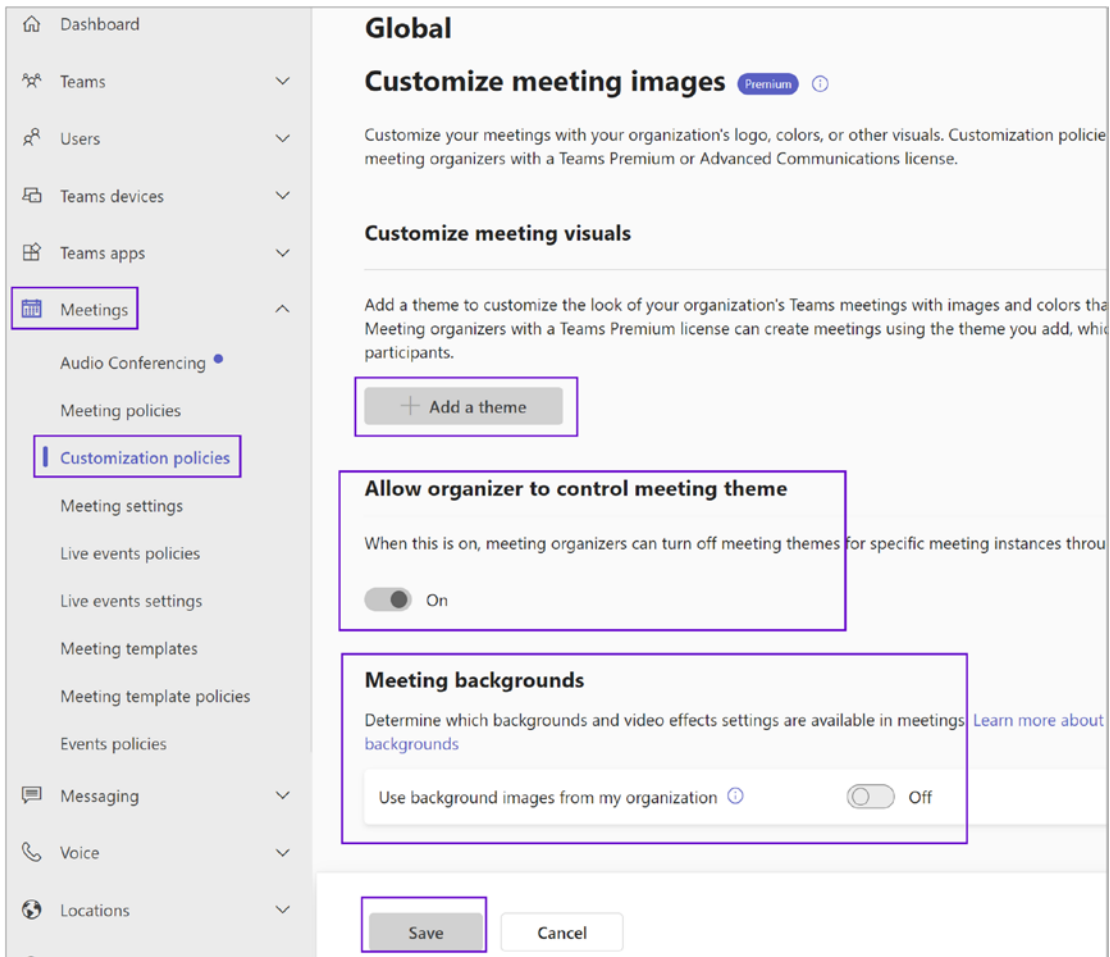


Figure 2-78. Customization policy

Managing Meeting Settings

Meeting settings allow you to customize meeting invitations, set up cross-cloud relationships, and manage network settings for all Teams meetings in your organization. Microsoft Teams provides meeting settings that determine whether anonymous users can join Teams meetings, customize meeting invitations, enable quality of service (QoS), and set port ranges for real-time traffic. If you change any of these meeting settings, the changes will be applied to all Teams meetings that users schedule within your organization. There are three main settings.

Participants

This option determines whether anonymous participants can join a meeting. Anonymous participants are users who can join without logging in, as long as they have the link for the meeting. An admin can turn on this feature per the organization requirements. To enable anonymous users to join a meeting, log in to the Teams admin center and navigate to Meetings. Select Meeting Settings, and under Participants, turn on the “Anonymous users can join a meeting” option. Another option is “Anonymous users can interact with apps in meetings.”

Email Invitation

Microsoft allows organizations to customize meeting invitations with their company logo and support as well as legal URLs. Based on the organization’s needs and requirements, the meeting invitations can be customized and previewed before being applied to an organization’s settings. For example, Bloguc customized meeting invitations by adding their organization’s logo, links to their support website and legal disclaimer, and a text-only footer. To customize meeting invitations, log in to the Teams admin center and navigate to Meetings. Select Meeting Settings, and under Email Invitation you can add a logo URL, legal URL, help URL, and footer text. Figure 2-79 shows a preview for email invitation settings.

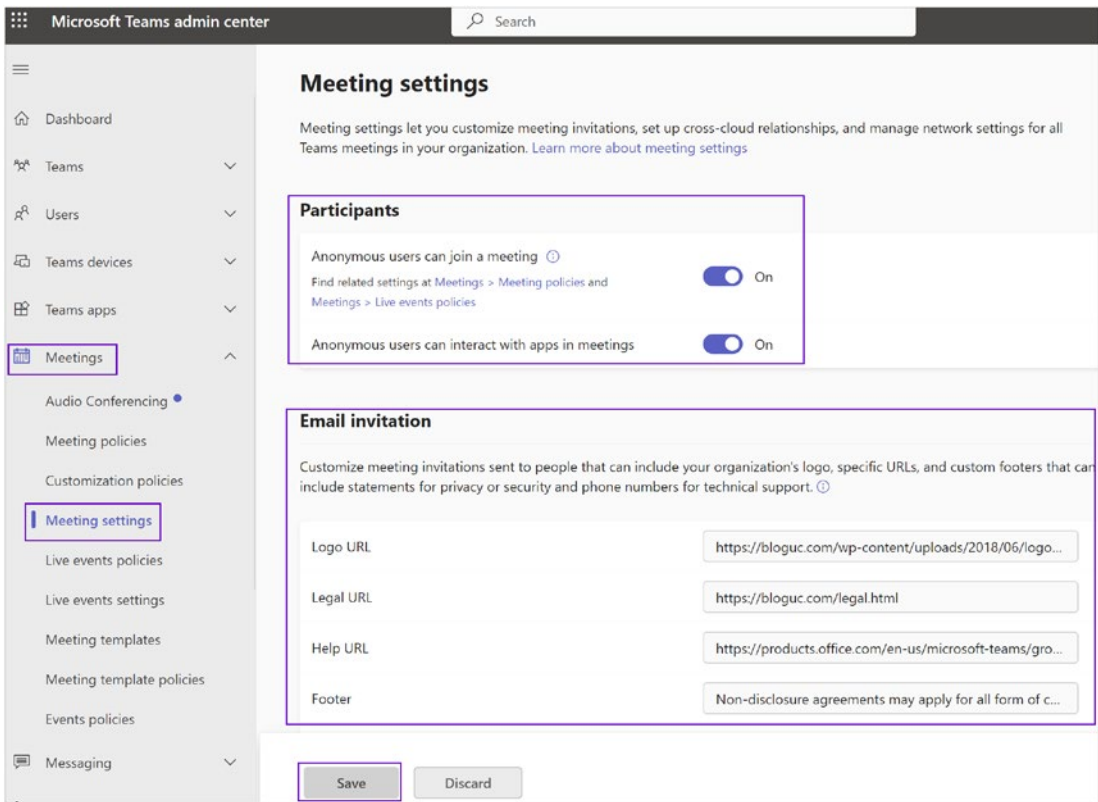


Figure 2-79. Participant setting and email invitation customization

Network

If you are using QoS to prioritize network traffic, you can enable QoS markers and set port ranges for each type of media traffic. It is important to note that if you enable QoS or change settings in the Microsoft Teams admin center for the Microsoft Teams service, you will also need to apply matching settings to all user devices and all internal network devices to fully implement the changes to QoS. When you turn on “Insert Quality of Service (QoS) markers for real-time media traffic,” all the real-time media traffic for meetings will be marked. If they have this marking, the network packets can be prioritized.

It is important to use port ranges to specify which ports to use for specific types of media traffic. Setting this to automatic mode would use any available ports within the 1024–65535 range. I recommend using the Specify Port Ranges option and using a smaller port range. Figure 2-80 shows all the recommended starting and ending port numbers with their media types.

Network

Set up how you want to handle Teams meetings real-time media traffic (audio, video and screen sharing) that flow across your network. ⓘ

Insert Quality of Service (QoS) markers for real-time media traffic On ⓘ

Select a port range for each type of real-time media traffic ⓘ

Specify port ranges
 Automatically use any available ports

Media traffic type	Starting port	Ending port	Total ports
Audio	50000	50019	20
Video	50020	50039	20
Screen sharing	50040	50059	20

Save Discard

Figure 2-80. Network and QoS settings

In summary, the Meetings tab in the Teams admin center is a comprehensive toolkit for managing and optimizing the meeting experiences within your organization. Given the importance of meetings in driving effective collaboration, decision-making, and productivity, it's crucial to manage these settings to fit your organizational needs.

Note The Live Event Policies and Live Event settings were described in the “Overview of Live Events” section in this chapter.

Meeting Templates

Meeting templates can be used to create meetings that are available to users with common needs or a common project. Meeting templates are available to all organizations including small to large business and educational organizations.

Note This setting is available only with Teams Premium.

Meeting Template Policies

Meeting template policies let you create and set up policies that control what templates people in your organization can see. You can use the Global (Org-wide default) policy and customize it, or you can create custom policies from scratch.

Note This setting is available only with Teams Premium.

Event Policies

Teams event policies are used to configure event settings on Teams, starting with webinars. You can use the Global (Org wide default) policy and customize it, or you can create custom policies and assign them to people who create, run, and manage events in your organization. Figure 2-81 shows event policy settings.

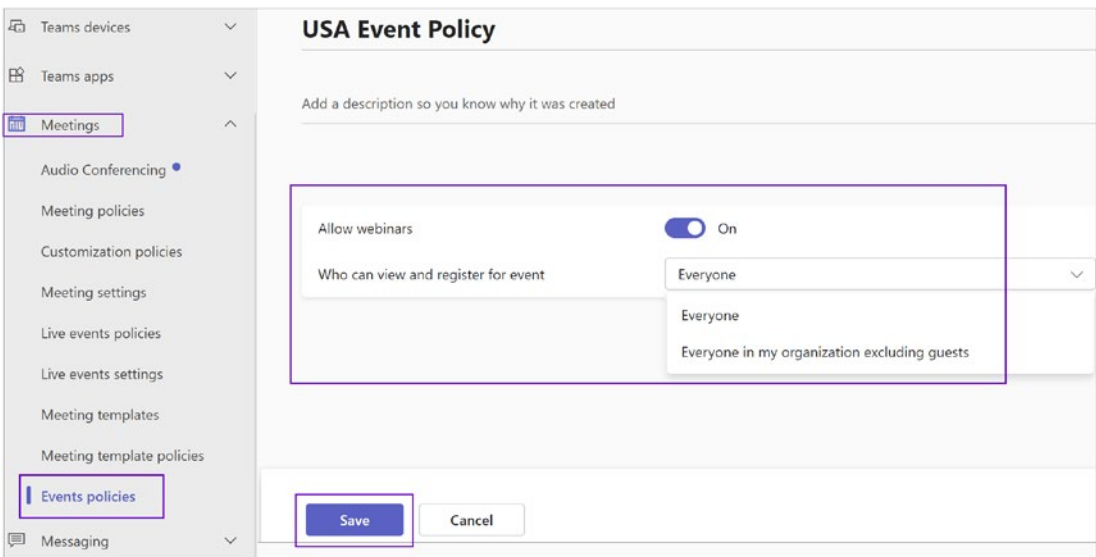


Figure 2-81. Teams events policy

Admin Center: Messaging Policies Tab

Microsoft Teams provides optimal chat capability through one-to-one chat, group chat, or channel chat. For this reason, Teams is often called a *chat-based workspace*. Teams not only provides chat capability but also provides granular control to manage the Teams

chat experience through Teams messaging policies that are used to control chat and channel messaging features for users such as the ability to delete sent messages, access to memes and stickers, or the ability for users to remove other users from a group chat.

Out of the box, all users are assigned to the Global (Org-wide default) policy. A Teams admin can create additional custom policies and assign them to individual users, but a user can be assigned to only one messaging policy at a time. Also, messaging policies can be used to activate or deactivate messaging features and to configure or enforce messaging settings. All messaging policies are managed from the Microsoft Teams admin center and through the PowerShell commands.

Note Any user can have only one messaging policy assigned at a time, regardless of policy type.

Some of these settings, such as using Giphys, can also be configured at the team level by team.

Creating New Messaging Policies

Messaging policies are used to control what chat and channel messaging features are available to users in Teams. You can use the Global (Org-wide default) policy or create one or more custom messaging policies for people in your organization.

By default, there will be one Global (Org-Wide default) messaging policy available that has been assigned to every user in your organization. If different settings for individual users are required, such as when an organization wants to deny regular users the ability to delete sent messages, a Teams admin must create a new messaging policy and assign it to a user.

To create a new messaging policy in the Teams admin center and assign it to a user, follow these steps:

1. Log in to the Teams admin center. In the left navigation pane, select Messaging Policies. Click +Add. In the top section under Messaging policies/Add window, enter the following information:
 - *New Messaging Policy*: A name for the policy.

- *Description:* A description for the policy.
- Turn on or off all settings as required, including allowing or blocking deletion of sent messages, read receipts, chat, Giphy content rating, URL preview, and so on. Figure 2-82 shows recommended settings, but the admin can customize the policy.

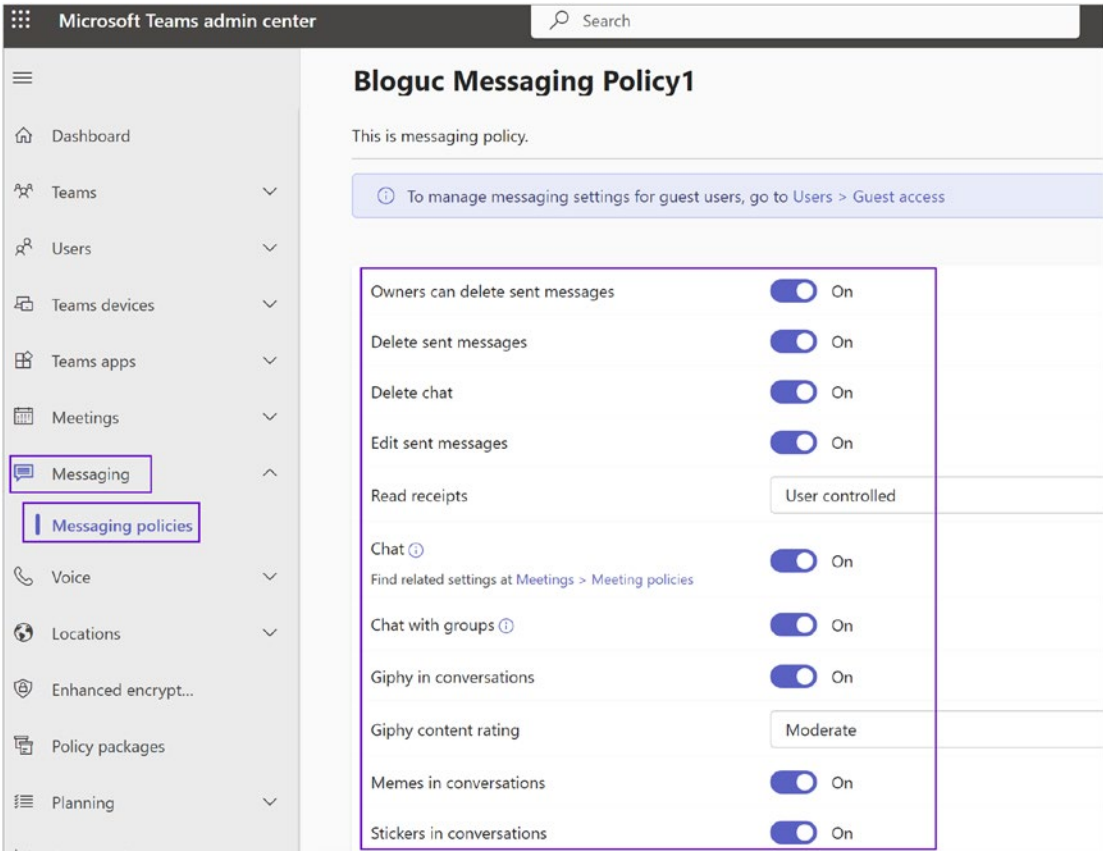


Figure 2-82. Messaging policy

The screenshot shows a settings window for a Microsoft Teams messaging policy. It contains two sections of settings, each enclosed in a purple box. The first section includes: URL previews (On), Report inappropriate content (On), Report a security concern (On), Translate messages (On), Immersive reader for messages (On), and Send urgent messages using priority notifications (On). The second section includes: Create voice messages (Allowed in chats and channels), On mobile devices, display favorite channels above recent chats (Enabled), Remove users from group chats (On), Text predictions (On), Suggested replies (On), Chat permission role (Restricted permissions), Users with full chat permissions can delete any message (Off), and Video messages (On). At the bottom, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a purple box.

URL previews	<input checked="" type="checkbox"/> On
Report inappropriate content ⓘ	<input checked="" type="checkbox"/> On
Report a security concern ⓘ	<input checked="" type="checkbox"/> On
Translate messages	<input checked="" type="checkbox"/> On
Immersive reader for messages	<input checked="" type="checkbox"/> On
Send urgent messages using priority notifications ⓘ	<input checked="" type="checkbox"/> On
Create voice messages	Allowed in chats and channels
On mobile devices, display favorite channels above recent chats	Enabled
Remove users from group chats	<input checked="" type="checkbox"/> On
Text predictions ⓘ	<input checked="" type="checkbox"/> On
Suggested replies ⓘ	<input checked="" type="checkbox"/> On
Chat permission role ⓘ	Restricted permissions
Users with full chat permissions can delete any message ⓘ	<input type="checkbox"/> Off
Video messages	<input checked="" type="checkbox"/> On

Save Cancel

Figure 2-82. (continued)

2. Once you have selected the desired settings, click Save to commit the policy setting and create the new messaging policy.
3. After a new messaging policy is created, it will be displayed in the Messaging Policies window, where it is ready for assignment to individual users. To assign the newly created policy to a user, you should perform the following steps:

- a. Log in to the Teams admin center, and then select Users. Select a user and open User Setting; then select the Policies tab. Click Edit beside Assigned Policies.
- b. Use the Messaging Policy drop-down menu to select the newly created messaging policy and then click Apply, as shown in Figure 2-83. The new messaging policy is now assigned to a user, and its configured settings will be applied after up to 24 hours.

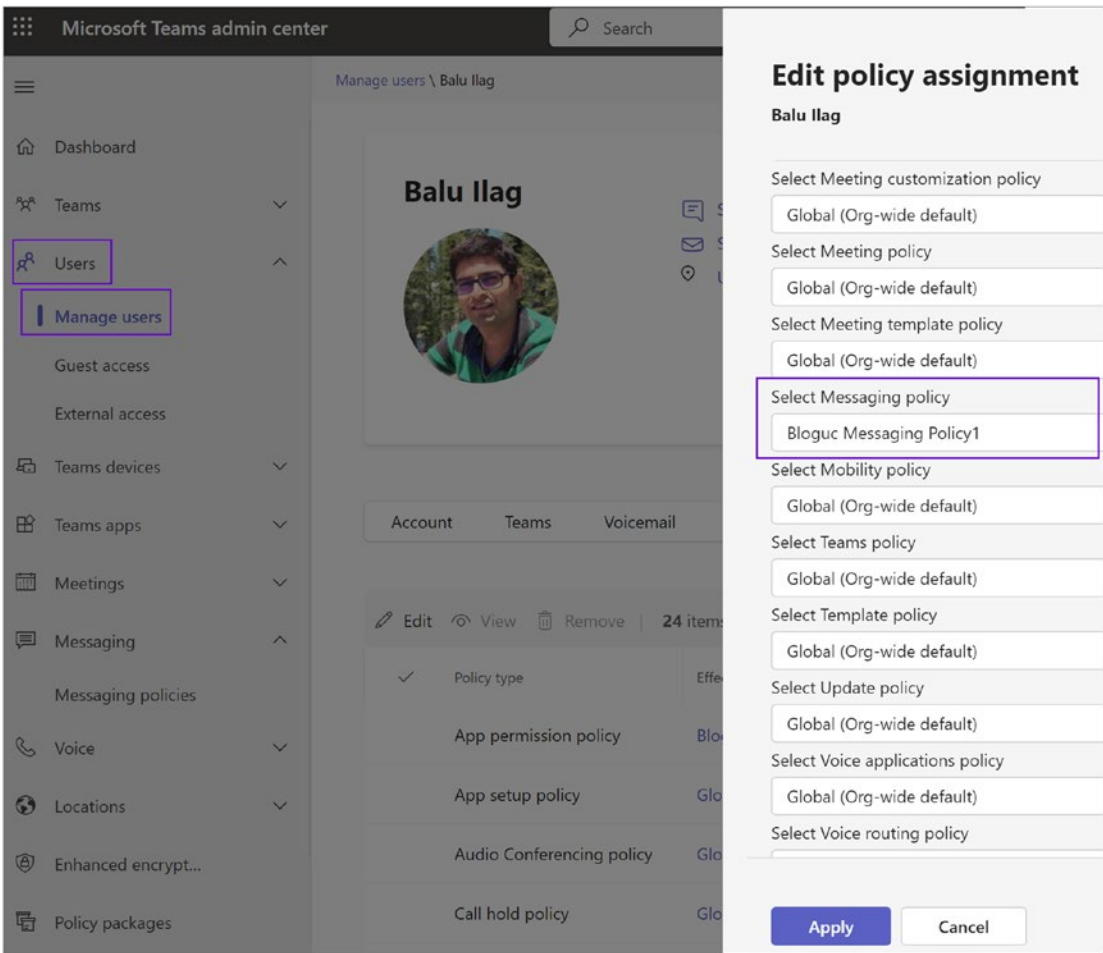


Figure 2-83. Messaging policy assigned to user

Modifying or Deleting Message Policies

When changes to an existing messaging policy are required or if the “Global policy” settings need to be changed, they can be edited, or in the case of custom policies, they can be deleted.

Note The default Global (Org-wide default) policy cannot be deleted, but it can be reset to default settings.

To modify policies or delete them, you should log in to the Teams admin center and then select Messaging Policies. Select the box for the policy that you want to modify or delete. You should then select one of the following options, as shown in Figure 2-84:

- Click Edit to delete the policy.
- Click Duplicate to create a copy of the selected policy with a “copy” suffix.
- Click Delete to remove the policy.

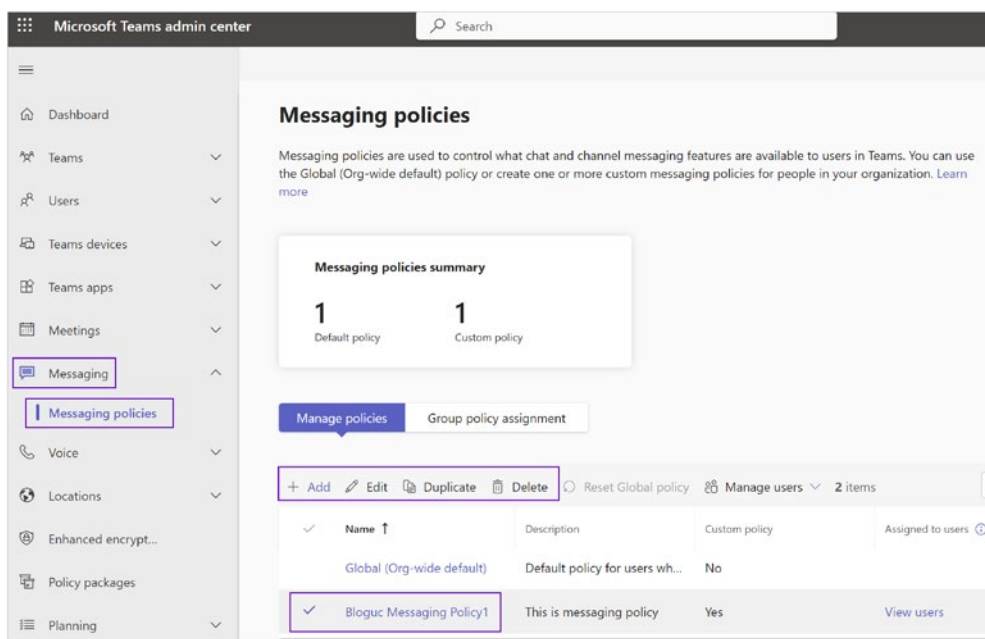


Figure 2-84. Modifying the messaging policy

Managing Messaging Policies Using PowerShell

As mentioned earlier, you can create and manage Teams messaging policies using PowerShell. The required commands to work with messaging policies are available in the Skype for Business Online module. Here is a list of the commands:

- `Get-CsTeamsMessagingPolicy`
- `New-CsTeamsMessagingPolicy`
- `Set-CsTeamsMessagingPolicy`
- `Grant-CsTeamsMessagingPolicy`
- `Remove-CsTeamsMessagingPolicy`

Here are examples to get the Global (Org-wide default) policy, create a new policy, modify a policy, and grant a policy to the user, respectively:

```
Get-CsTeamsMessagingPolicy Global
New-CsTeamsMessagingPolicy -Identity BlogucMessagingPolicy1 -AllowGiphy
>false -AllowMemes $false
Set-CsTeamsMessagingPolicy -Identity BlogucMessagingPolicy1 -AllowGiphy
>false -AllowMemes $false
Grant-CsTeamsMessagingPolicy -identity "Balu Ilag" -PolicyName
BlogucMessagingPolicy1
```

Admin Center: Voice Tab

The Microsoft Teams admin center's Voice tab is a centralized location for configuring and managing voice and calling features for your organization's Teams deployment.

Here's a rundown of its capabilities:

- **Phone numbers:** This section allows you to acquire, assign, and manage phone numbers for your users and services such as audio conferencing, auto attendants, and call queues.
- **Operator connect:** This feature allows you to integrate with and manage relationships with telephony operators for Public Switched Telephone Network (PSTN) connectivity.

- **Direct routing:** This feature allows you to integrate Microsoft Teams with your existing telephony infrastructure via Session Border Controllers (SBCs) and manage settings related to voice routes and PSTN usage records.
- **Calling policies:** This is where you define what calling features are available to Teams users. You can create and manage policies and assign them to users or groups.
- **Call hold policies:** These policies control the music or audio file that's played when a Teams user puts a call on hold.
- **Call park policies:** This capability lets you manage settings related to the "call park" feature, which allows users to put a call on hold and then retrieve it on a different device.
- **Caller ID policies:** These policies let you control how a user's phone number is displayed to others during a call, including options to display an alternate number or block the display of the number.
- **Dial plans:** Dial plans are sets of normalization rules that translate dialed phone numbers into a standard format for routing and authorization.
- **Emergency policies:** This section lets you manage settings related to emergency calling features, including dynamic location updates for emergency services.
- **Mobility policies:** These policies control what Teams Phone Mobile features are available to users.
- **Voice routing policies:** These policies are used to manage the routing of calls made through Direct Routing, including prioritization of PSTN usages and routing to specific SBCs.
- **Voicemail policies:** These control the available features for the voicemail service in Teams, including transcription, message duration, and other settings.

Each of these features provides a critical part of managing the overall voice and calling experience in Teams, ensuring users can communicate effectively and that the organization's telephony requirements are met.

The Voice tab includes several settings related to calling and phone usage for Microsoft Teams, as shown in Figure 2-85.

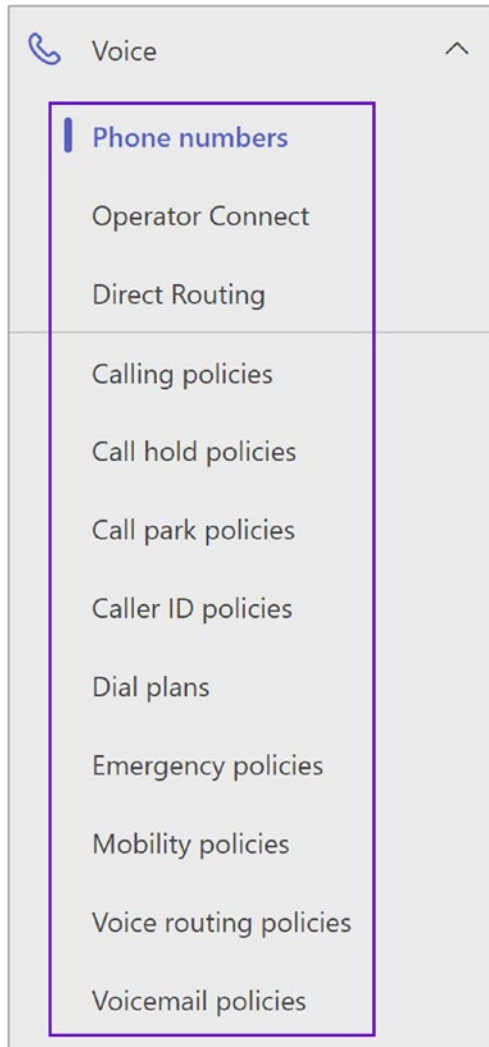


Figure 2-85. Teams Voice features

Phone Numbers

To set up calling features for users and services in your organization, you can get new numbers or port existing ones from a service provider. You can manage phone numbers including assigning, unassigning, and releasing phone numbers for people or for services such as audio conferencing, auto attendants, or call queues.

Phone Number Management

The Microsoft Teams admin center allows Teams admins to port their existing on-premise phone numbers, search for new numbers, and acquire new phone numbers from Microsoft 365 Phone System. In addition to acquiring new numbers, you can assign these new numbers to end users and resource accounts. Admins can manage locations for emergency calling and assign them to users. This means when you assign phone numbers to end users, they have their emergency location configured. When they make a call to emergency services, this location address can help them to get help quickly. Admins can see all order histories as well as updates to their records.

To add new phone numbers, follow this procedure:

1. Log in to the Teams admin center, and navigate to Voice. Select Phone Numbers and then click +Add to add a new phone number.
2. On the Phone Numbers/Get Phone Number page, enter the order name and a description.
3. Under Location And Quantity, select the country or region and then select appropriate number type and search location (if you have not added a location then you need add a location first to search). Specify the quantity and then click Next. In the example shown in Figure 2-86, the order name is Demo Order, the selected country is United States, the number type is user number, the location is HQ, the area code is 209, and the quantity is five. The number acquisition process takes some time, so be patient.

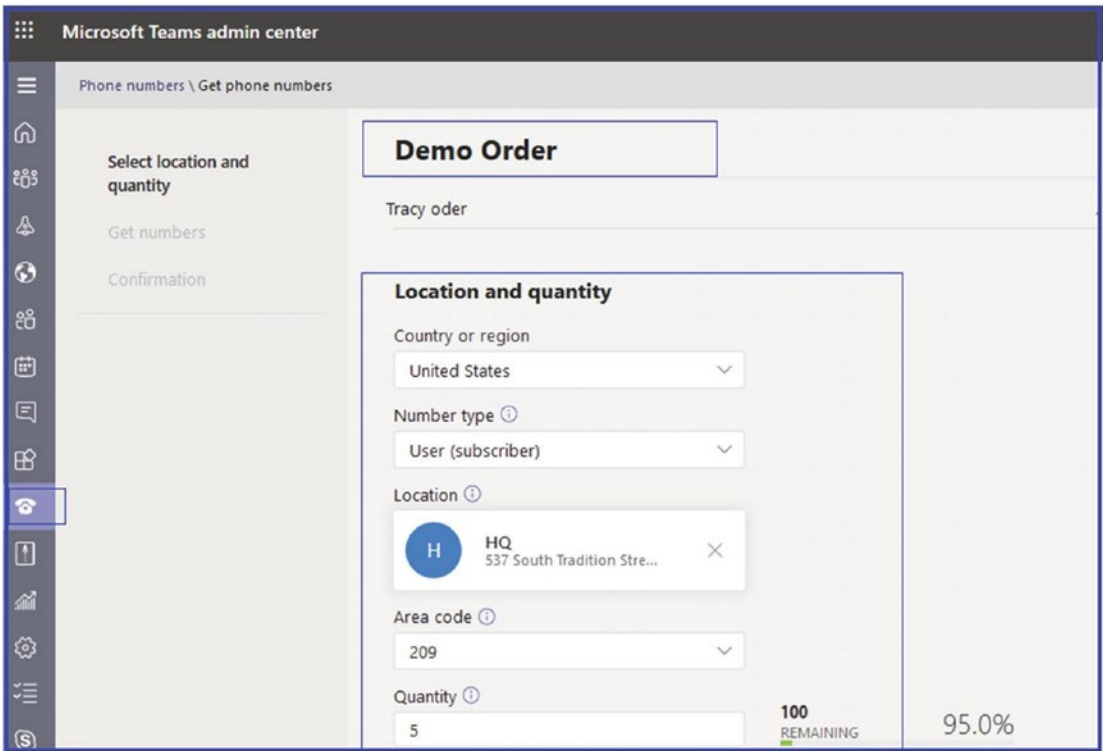


Figure 2-86. Phone numbers

4. On the next page, you will see the new number added and finally confirm.

Note If you are trying to acquire phone numbers without Phone System licenses, you will end up getting an error, because to acquire phone numbers and use them, you must have Phone System licenses.

Porting Phone Numbers

Admins have the ability to port phone numbers from an existing service provider into the Microsoft 365 Cloud Teams service. There are two processes for porting the phone numbers. The first is automated porting, which is supported for U.S.-based numbers only (Microsoft-developed API with carrier and partners to be able to automate the whole process from end to end). The other porting option is through a service desk, which is available for all porting scenarios through support.

To port through a service desk, you as the Teams admin can download a form that the service desk provides, fill it out, sign it, scan it, and email it to Microsoft.

1. To port a phone number, log in to the Teams admin center, and navigate to Voice. Select Phone Numbers and then click Port to port phone numbers.
2. On the Porting page, review the information before you start transferring your phone numbers. After you review it, we will walk you through the steps you need to complete the transfer of your numbers from your current service provider to Microsoft. When you're ready, click Next to continue (see Figure 2-87).

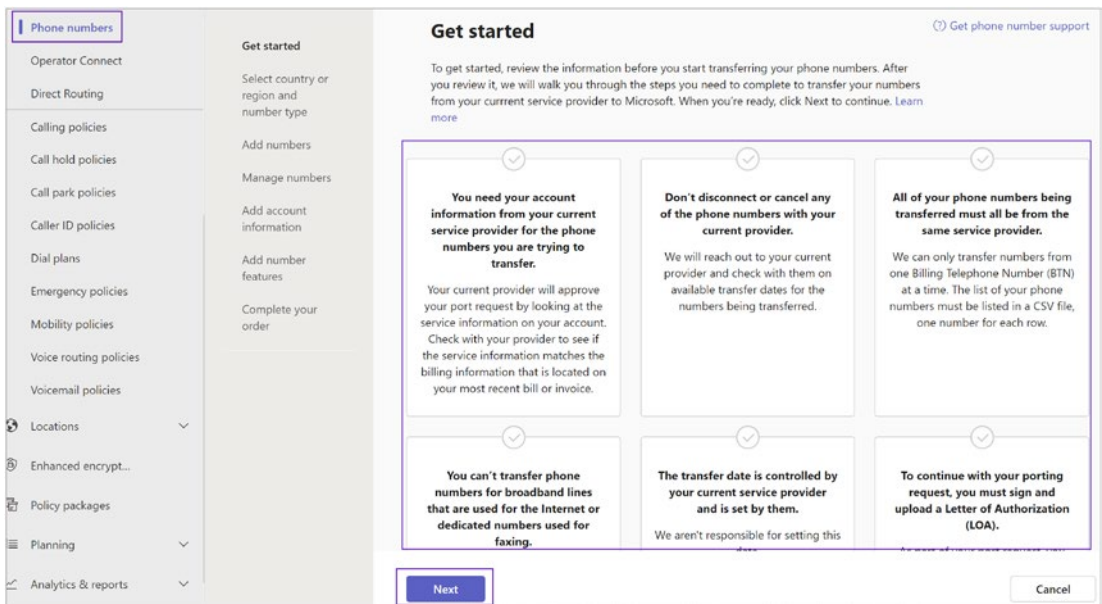


Figure 2-87. Porting the number

You can check the order history.

Operator Connect

Operator Connect allows you to manage partnerships with your phone operators. You can manage operators you already have a relationship with or view all operators to set up a partnership with a new operator.

Direct Routing

Microsoft Teams Direct Routing is a feature that allows organizations to connect their on-premises telecom infrastructure (like a PBX or SIP trunk) to Microsoft Teams. In other words, it connects your phone system to the Microsoft Teams environment using a Session Border Controller (SBC). This enables users to make and receive calls within Microsoft Teams using the organization’s existing telecom provider.

The benefit of Direct Routing is that it gives organizations greater control over their telephony solutions, such as the ability to use existing contracts with telecom providers, add capacity as needed, or implement advanced features that may not be supported by Microsoft’s Calling Plans.

Direct Routing allows the Teams admin to connect a supported SBC to the 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 provides another way to connect to the PSTN where customers interface existing PSTN services to Teams through an on-premises SBC.

If your organization has an on-premises PSTN connectivity solution (e.g., the Bloguc organization uses a ribbon SBC to connect an AT&T SIP trunk), direct routing enables you to connect a supported SBC to the Microsoft Phone System. Direct routing enables you to use any PSTN trunk with your Microsoft Phone System and configure interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and the Microsoft Phone System.

Figure 2-88 shows the connectivity from on-premises PSTN connectivity with a Microsoft Teams client using a Direct Routing capability.

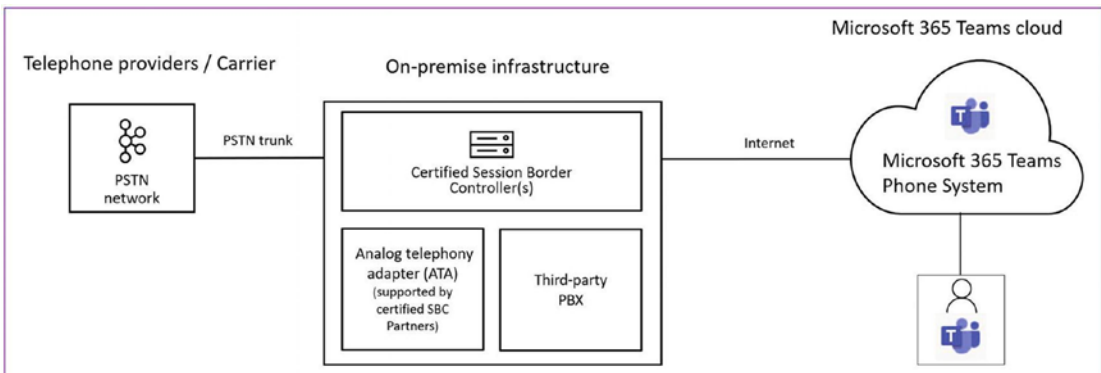


Figure 2-88. Teams Direct Routing high-level connectivity

Scenarios in Which You Can Use Direct Routing

As mentioned earlier, Direct Routing provides a way for the Teams admin to connect a supported SBC to the Microsoft Phone System to enable voice calling features (PSTN calls). Direct Routing can be deployed in organizations that want to leverage on-premises PSTN within the following scenarios:

- The Microsoft Calling Plan is not available in the organization's country or region. Thus far, the Microsoft Calling Plan is available in only some countries. You can visit <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> to see where Calling Plan is available.
- The organization requires a connection to third-party analog devices or call centers.
- The organization has an existing contract with a PSTN carrier and wants to continue to use on-premises PSTN.

Prerequisites for Planning or Deploying Direct Routing

As a Teams admin, you should confirm you have the infrastructure requirements in place to deploy a Direct Routing solution in your organization. There are multiple requirements that you must be aware of and understand before planning or implementing Teams Direct Routing.

- The first step is to check your existing SBC for supportability. Microsoft has published a supported SBC vendor list with their product and software version. Validate your SBC, as it must be one from a supported SBC vendor. Read more details at <https://docs.microsoft.com/en-US/microsoftteams/direct-routing-border-controllers>.
- SBC must have one or more telephony trunks connected. The SBC can also be connected to third-party PBXs or analog telephony adapters. On the other end, the SBC will be connected to the Microsoft Phone System through Direct Routing; for example, select PSTN carrier ► SBC ► Microsoft Teams Office 365 Cloud.

- You must have an Office 365 tenant where your organization’s Teams users are located or homed.
- To use Direct Routing capabilities, users must be homed in Microsoft Teams. In a hybrid environment, on-premises Skype for Business users cannot be enabled for Direct Routing voice in Microsoft Teams.
- Your domains must be configured to your organization’s Office 365 tenant; for example, Bloguc.com means the SBC FQDN looks like this: sbc1.bloguc.com. The default *.onmicrosoft.com domain cannot be used.
- The SBC must have a public DNS FQDN and a public IP address interface that will be used to connect SBC to Teams Office 365 Cloud.
- The SBC connection to the Teams Office 365 Cloud is secured, so you must have a public trusted certificate for the SBC that will be used for communication with Direct Routing.
- The SBC public IP address interface must be allowed to communicate to Teams Direct Routing over certain ports and protocols. This is the firewall requirement mentioned here.
 - sip.pstnhub.microsoft.com: Global FQDN; must be tried first.
 - sip2.pstnhub.microsoft.com: Secondary FQDN; geographically maps to the second priority region.
 - sip3.pstnhub.microsoft.com: Tertiary FQDN; geographically maps to the third-priority region.
 - Firewall IP addresses and ports for Direct Routing and Microsoft Teams media should be opened. Table 2-3 identifies the ports that should be opened.

Table 2-3. *Traffic Types and Related Ports*

Traffic Type	From	To	Source Port	Destination Port
SIP/TLS	SIP Proxy	SBC	1024–65535	Defined on the SBC
SIP/TLS	SBC	SIP Proxy	Defined on the SBC	5061

- The Media Transport Profile should allow TCP/RTP/SAVP and UDP/RTP/SAVP. The media traffic flows to and from a separate service in the Microsoft Office 365 Cloud. The IP range for Media traffic should include 52.112.0.0 /14 (IP addresses from 52.112.0.1–52.115.255.254).
- Specific to the Media traffic codec perspective:
 - The Direct Routing interface on the leg between the SBC and Cloud Media Processor (without media bypass) or between the Teams client and the SBC (if media bypass is enabled) can use the following codecs:
 - Non-media bypass (SBC to Cloud Media Processor): SILK, G.711, G.722, G.729
 - Media bypass (SBC to Teams client): SILK, G.711, G.722, G.729, OPUS
 - On the leg between the Cloud Media Processor and the Microsoft Teams client, media flows directly between the Teams client and the SBC, where either SILK or G.722 is used.
- Teams Direct Routing licensing requirement. Users of Direct Routing must have the following licenses assigned in Office 365 to use Teams Direct Routing capabilities:
 - Microsoft 365 Phone System (either part of E5 or add-on license on top of E1 or E5).
 - Microsoft Teams (from Microsoft 365 subscription plan, like E1, E3, E5, etc.).
 - Microsoft 365 Audio Conferencing (either part of E5 subscription or add-on license on top of E1 and E3) is required in scenarios where a Teams user in a call wants to add a PSTN user in a call through the Audio Conferencing service.

Now that you are aware of the requirements, let's move on to configuring Teams Direct Routing.

Configuring Microsoft Teams Direct Routing

For Teams Direct Routing configuration, as of this writing, Teams admins can perform Direct Routing configuration through the PowerShell command line, such as using `New-CsOnlinePSTNGateway` only. There is no option to configure Direct Routing through the Team admin center. Microsoft will be adding a Direct Routing configuration capability for Teams admins in the Teams admin center portal to perform the configuration of Direct Routing and control the PSTN trunk definitions to support customers' on-premises PSTN connectivity with Microsoft 365. Using the Teams admin center portal, admins will include voice route support and assigning on-premises telephone numbers (TNs); however, as of this writing, it is not available through the admin portal but can be done using the Teams PowerShell command line. I am assuming when you read this book you will see a Teams Direct Routing configuration option in the Teams admin center portal.

Let's configure Teams Direct Routing using Teams PowerShell:

1. Connect the SBC to the Teams Direct Routing service of the Phone System using Teams PowerShell.
 - a. To do so, first connect Teams Online PowerShell using the following PowerShell command:

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

- b. After you are connected to Microsoft Teams PowerShell, run the following command to pair the SBC to the Office 365 tenant:

```
New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort  
<SBC SIP Port> -MaxConcurrentSessions <Max Concurrent  
Sessions the SBC can handle> -Enabled $true
```

Here's an example:

```
New-CsOnlinePSTNGateway -Fqdn sbc1.bloguc.com -SipSignallingPort  
5061 -MaxConcurrentSessions 50 -Enabled $true
```

Note It is recommended that you set a maximum call limit in the SBC, using information that can be found in the SBC documentation. The limit will trigger a notification if the SBC is at capacity.

2. After pairing with the SBC, you must validate the SBC setting is expected. If not, then modify it using the `Set-CsOnlinePSTNGateway` command. Figure 2-89 shows an example of PSTN gateway details.

A screenshot of a PowerShell terminal window with a yellow background. The command `PS C:\> Get-CsOnlinePSTNGateway -Identity sbc1.bloguc.com` is entered at the prompt. The output lists various configuration parameters for the PSTN gateway, such as `Identity`, `InboundTeamsNumberTranslationRules`, `SipSignalingPort`, and `SendSipOptions`, each followed by its value.

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

Identity                               : sbc1.bloguc.com
InboundTeamsNumberTranslationRules     : {}
InboundPstnNumberTranslationRules     : {}
OutboundTeamsNumberTranslationRules    : {}
OutboundPstnNumberTranslationRules    : {}
Fqdn                                    : sbc1.bloguc.com
SipSignalingPort                       : 5061
FailoverTimeSeconds                    : 10
ForwardCallHistory                     : False
ForwardPai                             : False
SendSipOptions                         : True
MaxConcurrentSessions                  : 50
Enabled                                : True
MediaBypass                            : True
GatewaySiteId                          :
GatewaySiteLbrEnabled                  : False
FailoverResponseCodes                  : 408,503,504
GenerateRingingWhileLocatingUser      : True
PidfLoSupported                        : False
MediaRelayRoutingLocationOverride     :
ProxySbc                               :
BypassMode                             : None
```

Figure 2-89. Validating PSTN gateway details

Note Validate if `SendSipOptions` is set to `True` or not. If not, then modify it to `True` because it is important to send option requests from SBC. When Direct Routing sees incoming SIP Options, it will start sending outgoing SIP Options messages to the SBC FQDN configured in the Contact header field in the incoming Options message.

3. Once an Online PSTN gateway is created, work with your SBC vendor to configure your SBC for Teams Direct Routing. That includes installing a certificate on SBC, adding a new public IP interface or network address translation (NAT) and FQDN on your SBC, opening communication between the SBC public IP interface and the Teams SIP proxy, actual call routing configuration, and so on.
4. The next thing you need to do is enable users for Teams Direct Routing. That includes creating a user in Office 365 or synchronizing your on-premises user through Azure AD, connecting to Office 365 and assigning a Phone System license, ensuring that the user is homed in Teams Online, configuring the phone number, enabling enterprise voice and voicemail, and configuring voice routing. The route is automatically validated.
 - a. Once a user is available in Office 365 (Azure AD), then assign the licenses, including Microsoft Teams, Microsoft Phone System, and Teams Audio Conferencing, using the Office 365 admin center.
 - b. Once licenses are assigned, configure the phone number and enable enterprise voice and voicemail for the user using the following PowerShell command. Before running this command, you must connect to Teams Online PowerShell.

```
Set-CsUser -Identity "Balu Ilag" -OnPremLineURI  
tel:+12092034567 -EnterpriseVoiceEnabled  
$true -HostedVoiceMail $true
```

Note If the user's phone number is managed on-premises, use on-premises Skype for Business Management Shell or Control Panel to configure the user's phone number.

- c. Create and assign a voice routing policy to the user including an Online voice routing policy. To create a voice routing policy, PSTN usages, and so on, refer the Microsoft documentation at <https://docs.microsoft.com/en-US/microsoftteams/direct-routing-configure>.
- d. Once the Online Voice routing policy is available, connect to Skype for Business Online PowerShell and assign the online voice routing policy to the user. Refer to the following PowerShell command to assign the online voice routing policy:

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "Balu Ilag"  
-PolicyName "Bloguc-CA-International"
```

Managing Teams Direct Routing

The Teams Direct Routing dashboard is the place where you see all your SBC configurations. Basically, this enumerates all the SBC configurations in the tenant with multiple data points on connectivity and quality with usage information. Every option has its help information associated with it, which helps the administrator check, test, and remediate any issues. The example in Figure 2-90 shows the Direct Routing dashboard with three SBCs. Two out of three SBCs are shown as active; however, there was no call made in the last 24 hours, so it displays as orange. There is one inactive SBC (sbc3.bloguc.com); the red mark means the SBC does have an issue that the admin has to address.

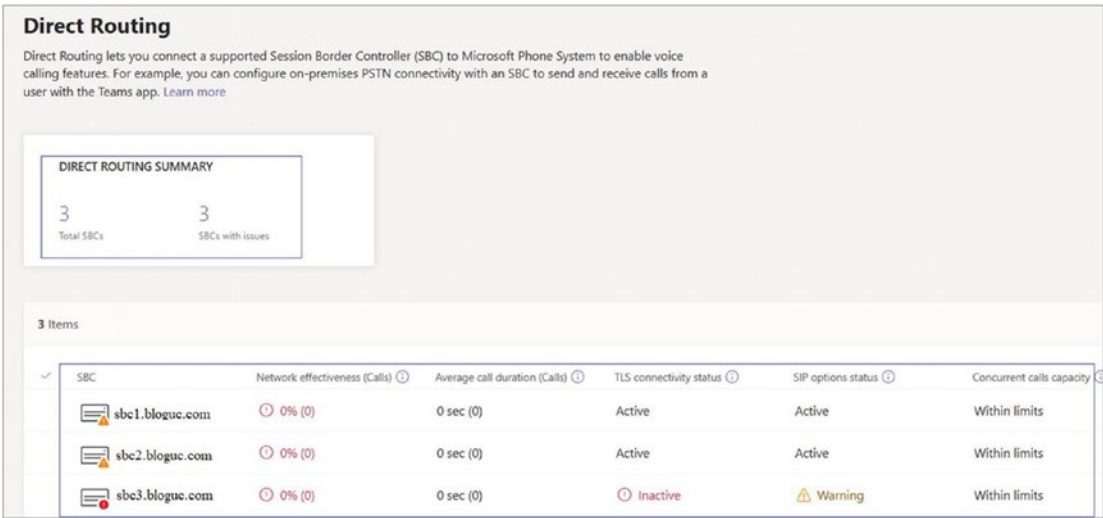


Figure 2-90. Teams Direct Routing dashboard

When you click `sbc1.bloguc.com`, it shows the statistics regarding calls, network parameters, and concurrent calls happening through this SBC, as displayed in Figure 2-91.



Figure 2-91. Teams Direct Routing SBC view

Best Practices for Implementing Teams Direct Routing

Here are some best practices for implementing Teams Direct Routing:

- **Ensure you have the necessary license and subscription:** Before you begin, you must have the right Office 365 license with Microsoft Teams and Phone System add-on. Understanding what is covered in your subscription can help you anticipate costs and configure the system accurately.
- **Choose the right SBC:** The SBC is an essential element in Direct Routing as it acts as an intermediary between your telecom provider and Teams. Microsoft has a list of certified SBCs. Choose one that suits your needs and budget.
- **Plan and configure network infrastructure:** Your network should have sufficient capacity to handle voice traffic. In addition, latency, packet loss, and jitter should be minimized to provide good call quality. You should also set up quality of service (QoS) rules to prioritize voice traffic.
- **Secure the connection:** Be sure to secure the connection between your SBC and Microsoft Teams. This could be achieved through Transport Layer Security (TLS) and secure Real-Time Transport Protocol (SRTP).
- **Number management:** Make sure you have a clear plan for managing and assigning telephone numbers to users. If you're porting numbers from an existing system, carefully plan the porting process to minimize disruption.
- **Emergency services:** Be aware of the rules in your country regarding provision of location information for emergency calls. You'll need to configure emergency addresses and locations in the Microsoft Teams admin center.
- **Test before going live:** Always thoroughly test your setup before going live. Make a few test calls to ensure that inbound and outbound calling works correctly. Test call quality and make sure that all call handling features work as expected.

- **Provide training:** Microsoft Teams might be new to many users. Ensure you provide adequate training and documentation to help them understand how to make and receive calls and use call handling features.
- **Monitoring and troubleshooting:** After implementation, use the Call Quality Dashboard and other monitoring tools provided by Microsoft to keep an eye on your system. This will help you spot any potential issues before they become major problems.
- **Create a disaster recovery plan:** While Teams and Direct Routing are quite reliable, it's always good to have a plan in place in case something goes wrong. This could involve having a backup SBC or having a failover procedure to an existing PBX or other phone system.

By following these best practices, you can ensure a smooth implementation of Microsoft Teams Direct Routing and provide your users with a high-quality and reliable voice service.

Calling Policies

Calling policies are used to control what calling features are available to people in Teams. You can use the Global (Org-wide default) policy and customize it or create one or more custom calling policies for people who have phone numbers in your organization.

Calling Policy Settings

The following are the settings:

- *Make Private call:* This setting controls all calling capabilities in Teams. Turn this setting off to turn off all calling functionality in Teams.
- *Cloud recording for calling:* This setting controls whether users can record calls. This setting is off by default.
- *Transcription:* This setting controls whether the transcription of calls is available for your users. This setting is off by default.

- *Routing for PSTN calls:* This setting controls how inbound PSTN calls should be routed. These PSTN calls can be sent to voicemail, sent to unanswered settings, or use default call routing, or you can allow your users to decide. “Use default settings” is on by default.
- *Routing for federated calls:* This setting controls how inbound federated calls should be routed. These federated calls can be sent to voicemail, sent to unanswered settings, or use default call routing. “Use default settings” is on by default. Federated calls are calls that don’t originate from the PSTN and that are outside your tenant.
- *Call forwarding and simultaneous ringing to people in your organization:* This setting controls whether incoming calls can be forwarded to other users or can ring another person in your organization at the same time. This setting is on by default.
- *Call forwarding and simultaneous ringing to external phone numbers:* This setting controls whether incoming calls can be forwarded to an external number or can ring an external number at the same time. This setting is on by default.
- *Voicemail for inbound calls:* This setting enables inbound calls to be sent to voicemail. The default setting is “Let users decide.” Valid options are as follows:
 - *On Voicemail:* This is always available for inbound calls.
 - *Off Voicemail:* This isn’t available for inbound calls.
 - *Let users decide:* Users can determine whether they want voicemail to be available.
- *Inbound calls can be routed to call groups:* This setting controls whether incoming calls can be forwarded to a call group. This setting is turned on by default.
- *Delegation for inbound and outbound calls:* This setting enables inbound calls to be routed to delegates, allowing delegates to make outbound calls on behalf of the users for whom they have delegated permissions. This setting is turned on by default.

- *Prevent toll bypass and send calls through the PSTN:* Turning on this setting sends calls through the Public Switched Telephone Network (PSTN) and incurs charges rather than sending them through the network and bypassing the tolls. This setting is off by default.
- *Music on hold for PSTN calls:* This setting allows you to turn on or turn off music on hold when a PSTN caller is placed on hold. It's turned on by default. This setting doesn't apply to call park and boss delegate features.
- *Busy on busy during calls:* Busy on busy during calls (also called *busy options*) lets you configure how incoming calls are handled when a user is already in a call or conference or has a call placed on hold. New or incoming calls can be rejected with a busy signal or can be routed accordingly to the user's unanswered settings. Regardless of how their busy options are configured, users in a call or conference or those with a call on hold are not prevented from initiating new calls or conferences. This setting is set to *Off* by default.
 - *Off:* No busy option is enabled, and new or incoming calls can still go to the user while the user is already in a call.
 - *On:* New or incoming calls will be rejected with a busy signal.
 - *Use unanswered settings:* The user's unanswered settings will be used, such as routing to voicemail or forwarding to another user.
 - *Let users decide:* Users can determine their busy options choice from call settings in the Teams app.
- *Web PSTN calling:* This setting enables users to call PSTN numbers using the Teams web client. This setting is on by default.
- *Real-time captions in Teams calls:* This setting controls whether real-time captions in Teams calls are available for your users. This setting is turned on by default.
- *Automatically answer incoming meeting invites:* This setting controls whether incoming meeting invites are automatically answered. It's turned off by default. Keep in mind that this setting applies only to incoming meeting invites. It doesn't apply to other types of calls.

- *Spam filtering*: This setting allows you to control the type of spam filtering available on incoming calls. This setting is on by default. This setting has three options.
 - *On*: Spam filtering is fully enabled. Both Basic and Captcha Interactive Voice Response (IVR) checks are performed. If the call is considered spam, the user gets a “Spam Likely” notification in Teams.
 - *On without IVR*: Spam filtering is partially enabled. Captcha IVR checks are disabled. A “Spam Likely” notification appears. A call might get dropped if it gets a high score from Basic checks.
 - *Off*: Spam filtering is completely disabled. No checks are performed. A “Spam Likely” notification doesn’t appear.
- *SIP devices can be used for calls*: This setting enables users to use a SIP device to make and receive calls. This setting is turned off by default.
- *Open apps in browser for incoming PSTN calls*: This setting controls whether apps are automatically opened in the browser for incoming PSTN calls to your users. This can be used to pass the phone number of an inbound caller to an app to find the associated customer record while the call is taking place. This setting is off by default.

If turned on, a link to the app needs to be given in the “URL to open apps in browser for incoming PSTN calls” box. You can use the {phone} placeholder to pass the phone number (in E.164 format) to the provided URL. Or, you can give a generic URL without any placeholder. This setting simply launches the listed URL. Figure 2-92 shows the calling policy settings.

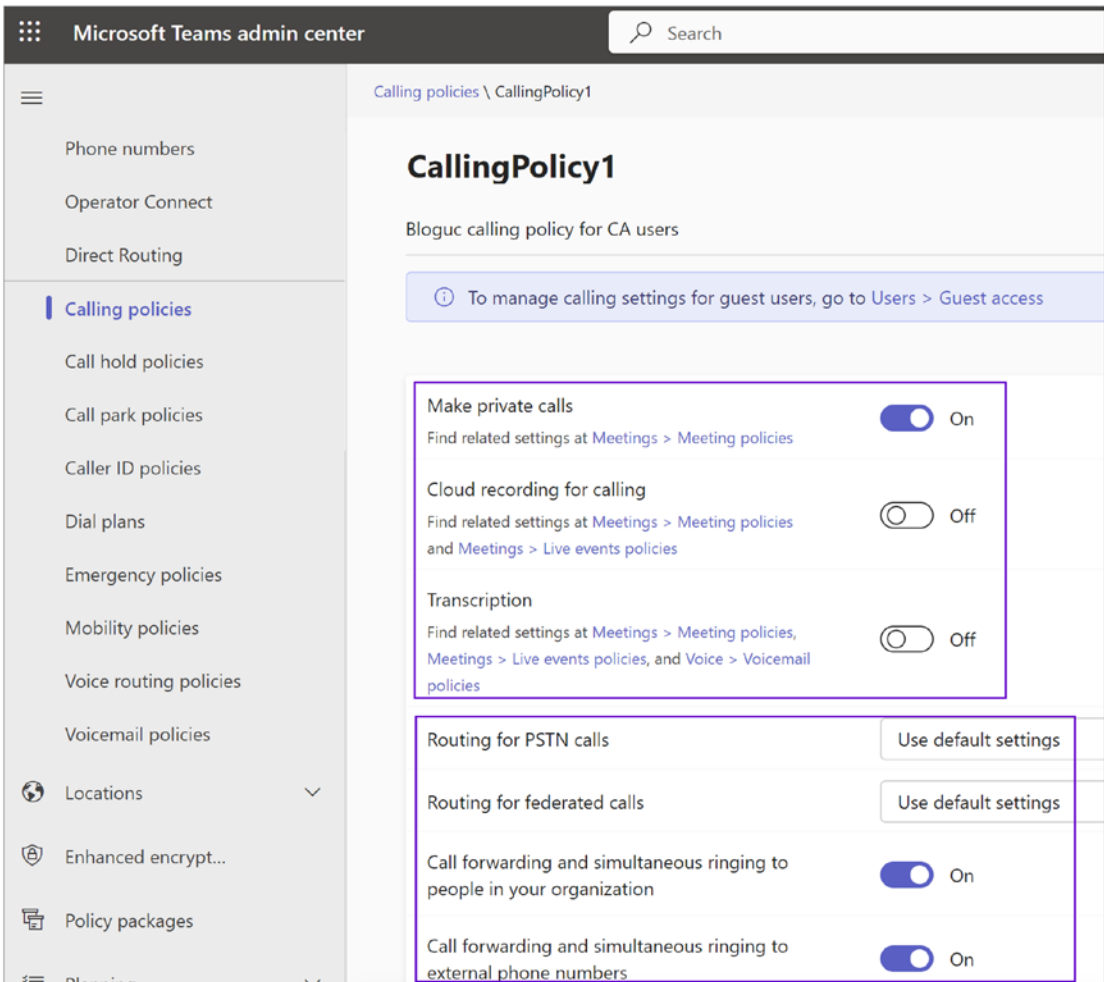


Figure 2-92. Teams Calling Policy settings

Vicemail for inbound calls	Let users decide	▼
Inbound calls can be routed to call groups	<input checked="" type="checkbox"/> On	
Delegation for inbound and outbound calls	<input checked="" type="checkbox"/> On	
Prevent toll bypass and send calls through the PSTN	<input checked="" type="checkbox"/> On	
Music on hold for PSTN calls	<input checked="" type="checkbox"/> On	
Busy on busy during calls ⓘ	On	▼
Web PSTN calling	<input checked="" type="checkbox"/> On	
Real-time captions in Teams calls <small>Find related settings at Meetings > Meeting policies</small>	<input checked="" type="checkbox"/> On	
Automatically answer incoming meeting invites	<input type="checkbox"/> Off	
Spam filtering	On	▼
SIP devices can be used for calls	<input type="checkbox"/> Off	
Open apps in browser for incoming PSTN calls	<input type="checkbox"/> Off	

Save Cancel

Figure 2-92. (continued)

Call Hold Policies

Call hold policies are used to control the audio file that's played when a Teams user puts a caller on hold. You can use the Global (Org-wide default) policy or create custom call hold policies for users that have phone numbers in your organization. Figure 2-93 shows the custom call hold policy settings.

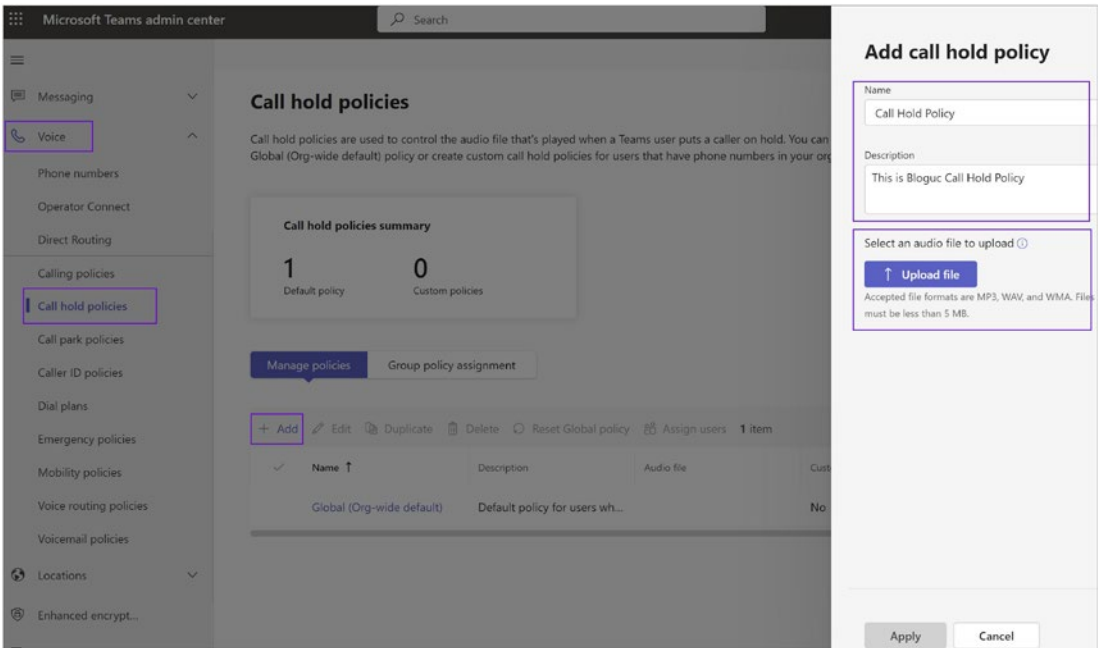


Figure 2-93. Teams call hold policies

Call Park Policies

Call parking allows users to put a call on hold and retrieve the call from a different device within the organization. Call Park policies allow a Teams administrator to control which users are enabled to use call park and make other call park setting changes for them. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies and assign them to users.

It is important to know that the call park feature is available in Teams-only mode. That enables a user to place a call on hold in the Teams service in the cloud. For example, a user’s phone battery is running low, so the user decides to park a call and then retrieve the call from a Teams desk phone. To park and retrieve calls, a user must be an Enterprise Voice user, and the Teams administrator must have granted the user a call park policy. The call park feature is disabled by default, but an admin can enable it for users and create user groups using the call park policy. Figure 2-94 shows Call Park policy with available options. You can configure call park options through PowerShell such as with `New-CsTeamsCallParkPolicy`. Here’s an example:

```
New-CsTeamsCallParkPolicy -Identity "HelpdeskPolicy" -AllowCallPark
$true -PickupRangeStart 500 -PickupRangeEnd 1500 -ParkTimeoutSeconds 600
```

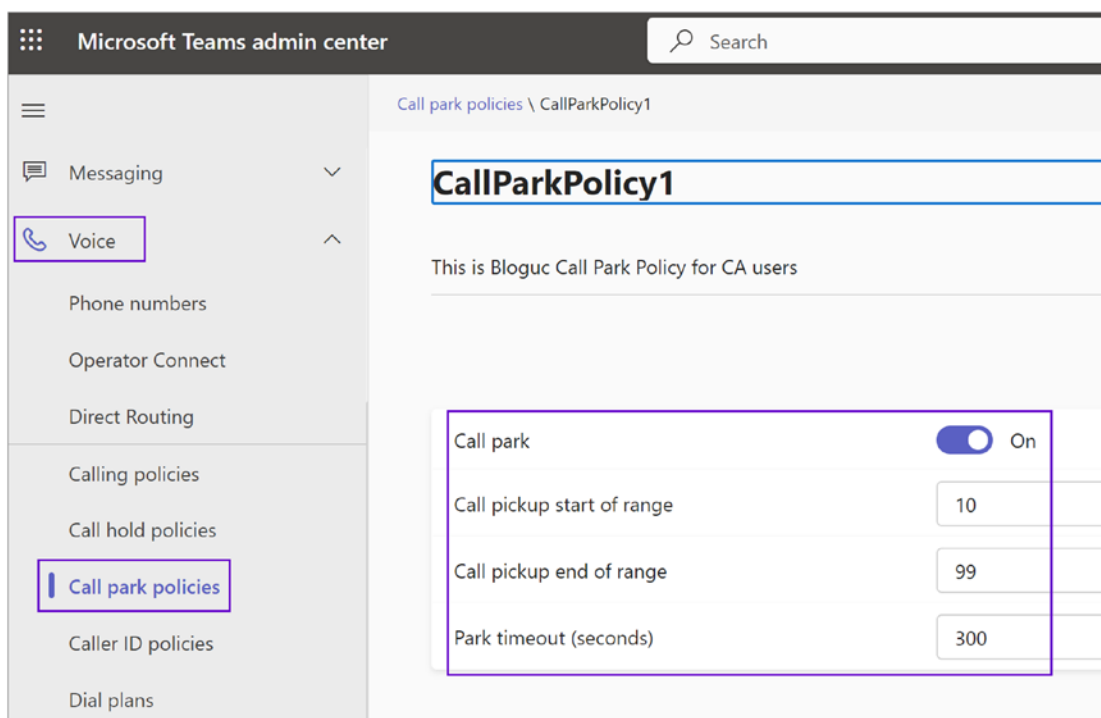


Figure 2-94. Teams call park policies

Caller ID Policies

Caller ID policies are used to change or block the caller ID (also called a calling line ID) for users. By default, the user's phone number is displayed when a call is made to a PSTN phone number such as a landline or mobile phone. You can use the Global (Org-wide default) policy and customize it or create a custom policy that provides an alternate number to display or to block any number from being displayed.

Caller ID is set up by default so that when a Teams user calls a PSTN phone, their phone number is displayed. Likewise, the phone numbers of PSTN callers can be seen when they call a Teams user. A Teams admin can manage caller ID policies in the Microsoft Teams admin center in the Voice section, under Caller ID Policies. You can select the Global (Org-wide default) policy or create custom policies according to your organization preferences and then assign them to users. If you do not create a policy, the users within the organization will by default have the Global policy assigned.

Creating a Custom Caller ID Policy

To create custom caller ID policy, follow these steps:

1. Log in to the Teams admin center and navigate to Voice. Select Caller ID Policies and then click +Add.
2. On the New Caller ID Policy page, enter a policy name and description for the policy and then configure the following policy settings:
 - *Block Incoming Caller ID*
 - *Override The Caller ID Policy*
 - *Replace The Caller ID With:* Display the user’s number; set a service phone number to display as the caller ID or display the caller ID as anonymous.
 - *Replace the Caller ID With This Service Number:* Use this setting to replace the caller ID. This option is available when you select Service Number in the “Replace caller ID with” field. Figure 2-95 shows these Caller ID settings.

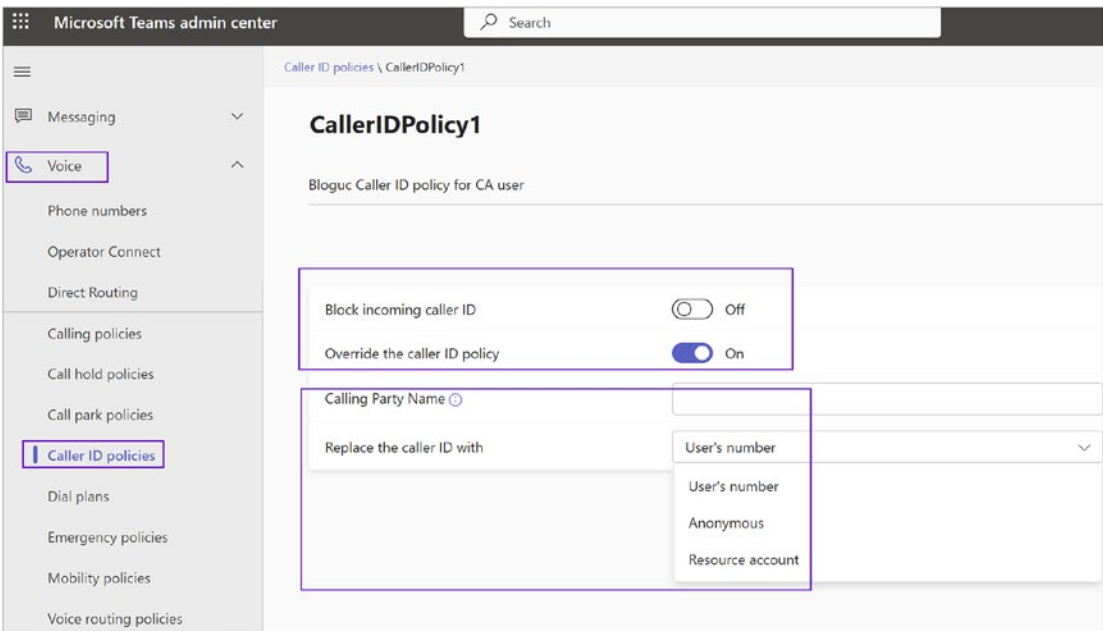


Figure 2-95. Caller ID policy

3. Once you are done configuring the caller ID settings, click Save.
4. Assign the policy to a user or group.

Dial Plans

A dial plan is a configuration applied to a user's phone in Microsoft Teams that influences how the phone number is interpreted and dialed out. Dial plans can be user-level or service-level (applied to everyone in your organization).

Microsoft Teams uses the E.164 format by default for phone numbers, but with dial plans, you can support other formats that might be more familiar or intuitive to your users. This is particularly useful for organizations that operate in countries where the local dialing habit might be different from the E.164 standard.

Here are some ways a dial plan is useful:

- **User experience:** Dial plans can make the dialing process more intuitive for your users. For instance, they might be used to dialing local numbers without the area code. A dial plan can be configured to automatically add the area code when they dial a local number.
- **Support for extension dialing:** Dial plans can be used to support extension dialing within your organization. For instance, a user might dial a four-digit extension, and the dial plan can translate this into a full phone number.
- **Normalization rules:** Dial plans consist of normalization rules that define how phone numbers expressed in various formats are interpreted (normalized) to the standard E.164 format. This provides flexibility and ensures consistency in how numbers are dialed within your organization.
- **Efficiency:** With a dial plan, users don't have to remember to dial in a specific format. They can dial as they usually would, and the dial plan will ensure the number is correctly interpreted. This can increase efficiency and reduce errors in dialing.

However, configuring and managing dial plans can be complex, particularly for large organizations. It's important to carefully plan your dial plan configuration to ensure it meets the needs of your users and aligns with your overall telephony strategy. Basically, using PowerShell you write a regular expression (RegEx), which is used to translate a dialed number to something that can be routed over PSTN.

Now, however, dial plans are available in the Teams admin center. There is a Global (Org-wide) dial plan that will be applied to all users in the Teams tenant or those who don't have custom dial plan applied. A custom dial plan allows you to codify users' dialing habits for each city or country, similar to handling voice routing policies.

Another important thing to understand is that normalization follows precedence. This means the first rule gets applied first if it matches; otherwise, it will go to the next one, and so on. If nothing matches, then it will give an error with no match found and call processing will stop, resulting in a failed phone call. That is why dial plans are essential in phone call routing.

Fundamentally, a dial plan is a set of rules that translate a phone number that a user dials into a standard E.164 number for call authorization and routing. You can use the Global (Org-wide default) dial plan that is created or create one or more custom dial plans for people in your organization. You can use the Global (Org-wide default) dial-plan policy as a basis to modify or create a custom dial-plan. Figure 2-96 shows a default dial plan.

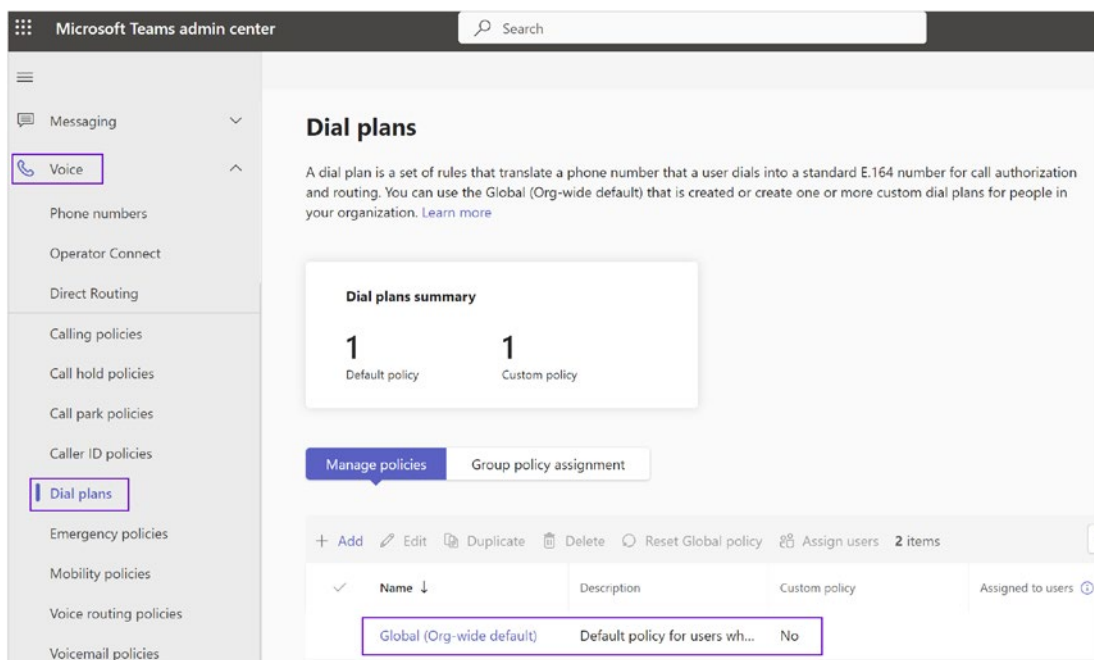


Figure 2-96. *Default dial plan policy*

Creating a Custom Dial Plan

To create custom dial plan, follow this procedure:

1. Log in to the Teams admin center, and then navigate to Voice. Select Dial Plans and then click +Add. Enter a name and description for the dial plan.
2. On the Dial Plan/Add page, under Dial Plan Details, specify an external dialing prefix if users need to dial one or more additional leading digits (e.g., 9) to get an external line. To do this, in the External Dialing Prefix box, enter an external dialing prefix (e.g., 9). The prefix can be up to four characters (including #, *, and 0–9). In Figure 2-97 the external dialing prefix is set to 9.
3. Set the Optimized Device Dialing option to on. If you specify an external dialing prefix, you must also turn on this setting to apply the prefix so that calls can be made outside your organization. This setting is shown in Figure 2-97.

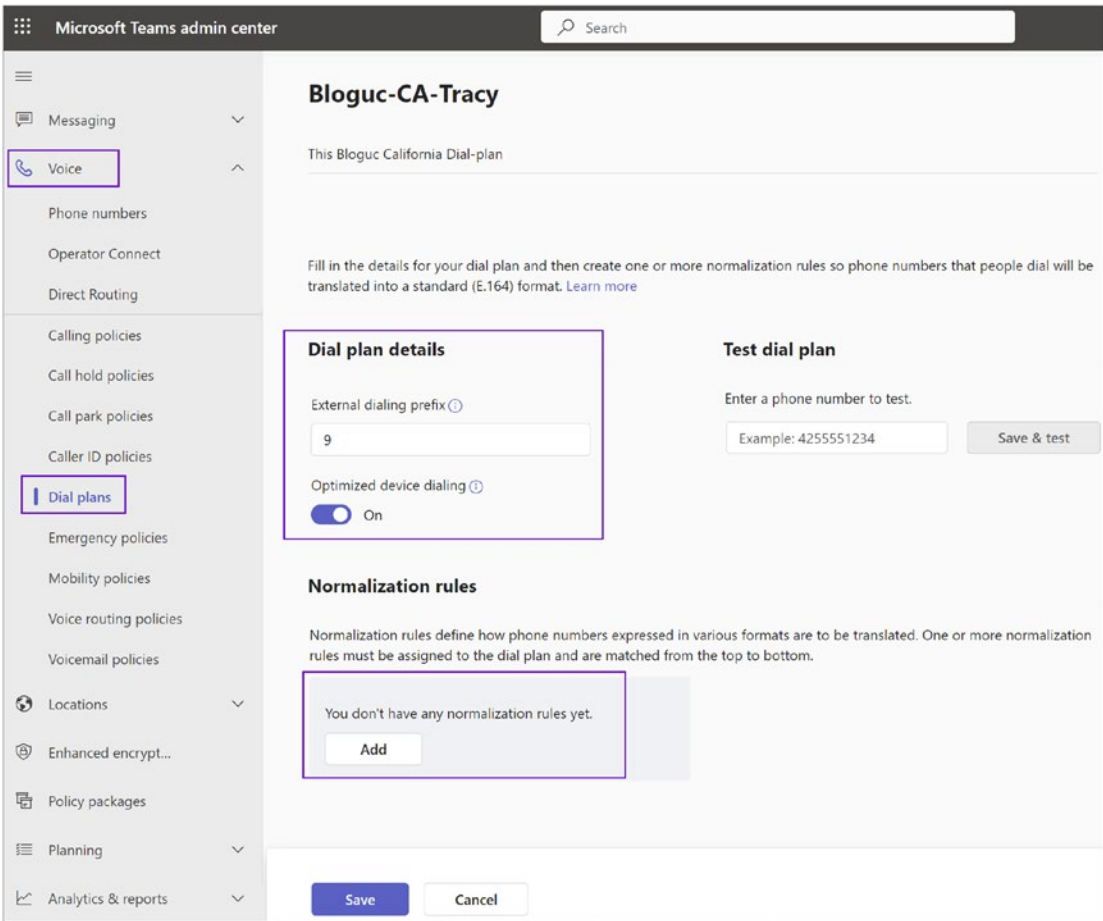


Figure 2-97. *Configuring a dial plan*

4. Under Normalization Rules, configure and associate one or more normalization rules for the dial plan. Each dial plan must have at least one normalization rule associated with it. To do this, follow this procedure.
 - a. To create a new normalization rule and associate it with the dial plan, click Add. You can then define the rule. Figure 2-98 shows a normalization rule named NorthAmerica-West.

- b. To edit a normalization rule that is already associated with the dial plan, select the rule by clicking to the left of the rule name, and then click Edit. Make the changes you want, and then click Save.
 - c. To remove a normalization rule from the dial plan, select the rule by clicking to the left of the rule name, and then click Remove.
5. Arrange the normalization rules in the order you want. Click Move Up or Move Down to change the position of rules in the list and then click Save to commit the changes.
6. After creating a dial plan, you must test it. Under “Test dial plan,” enter a phone number, and then click Test. Figure 2-98 shows five digits tested to make sure it normalizes correctly with E.164 format. For example, here the result shows +12096566625.

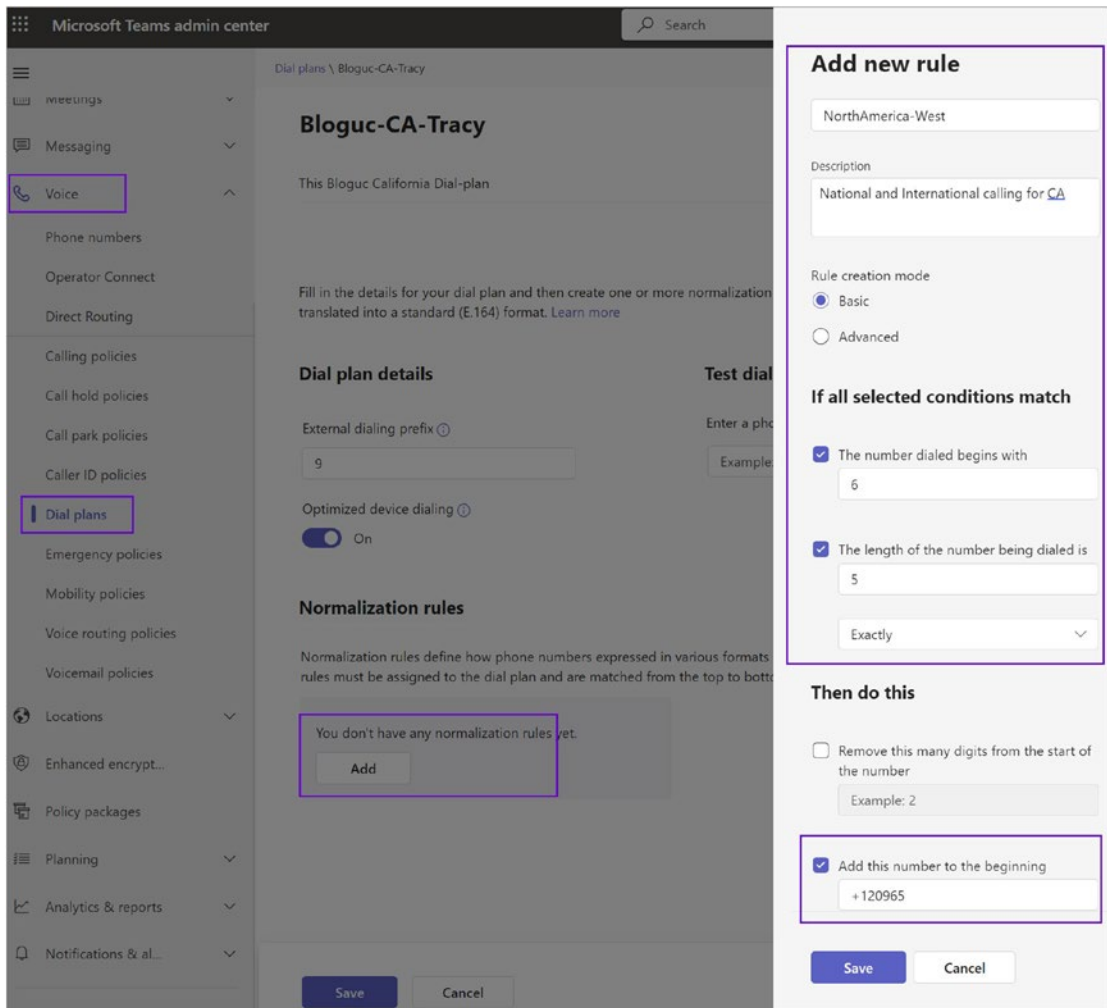


Figure 2-98. Normalization rule

Normalization Rule Types

Microsoft Teams provides two different types of normalization: basic and advanced. When you create a new dial plan, it will give you these two options. Basic is a basic option for conditions without regular expression, and it is an advanced option for complex dial plans with multiple conditions using regular expressions. Figure 2-99 shows the normalization rule type. Choose the normalization rule type that best fits your requirements.

Once your dial plan is ready, you as an admin can test the dial plan by dialing numbers, such as five-digit dialing, four-digit dialing, and so on. The next step is then to assign the dial plan to the user, by clicking Manage Users and then typing the username and assigning the dial plan to the end user.

Add new rule

Description

Add a friendly description so you know why it was created. For example:
"External numbers for NYC branch ..."

Basic Advanced

If all selected conditions match

The number dialed begins with
Example: "9"

The length of the number being dialed is
Example: "3"
Exactly

Then do this

Remove this many digits from the start of the number
Example: "2"

Add this number to the beginning
Example: "+1206"

Test this rule

Enter a phone number to test.
Example: "4255551234"

Figure 2-99. Normalization type selection

WHAT IS THE EXTERNAL DIALING PREFIX?

You can put in an external access prefix of up to four characters (including #, *, and 0–9) if users need to dial one or more additional leading digits (e.g., 9) to get an external line outside your organization. When you use this setting, you must also turn on optimized device dialing.

Assigning a Dial Plan to Users

To add users to a dial plan, first log in to the Teams admin center, and then navigate to Users. Select the desired user, and then click Policies. Under Assigned Policies, click Edit. Under Dial Plan, select the dial plan you want to assign. When you are finished adding users, click Apply. Repeat this step for each user you want to add. The example in Figure 2-100 shows assigning a dial plan to user Balu Ilag.

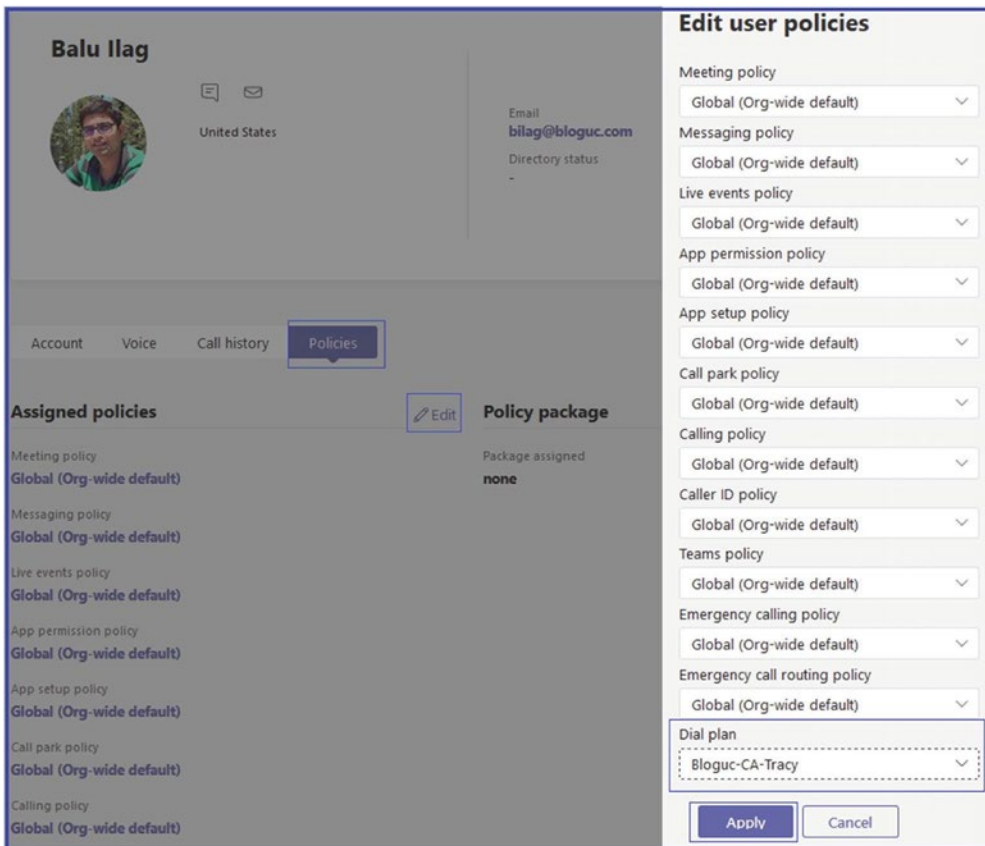


Figure 2-100. Assigning a dial plan to a user

Dial Plan Management and Creation Through Windows PowerShell

As a Teams admin, you have to manage dial plans and use them for call troubleshooting. Microsoft has provided multiple PowerShell commands that help you to manage dial plans. Before even running PowerShell commands, you must first connect your Windows PowerShell module to your Microsoft Teams tenant to the Microsoft 365 organization. You must have Microsoft Teams PowerShell module installed; you can use this link to Install Teams PowerShell module: <https://learn.microsoft.com/en-us/microsoftteams/teams-powershell-install>.

You can do that using the following PowerShell command, assuming you are not using MFA.

```
# When using Teams PowerShell Module
Install-Module -Name MicrosoftTeams -Force -AllowClobber
# Connect to Microsoft Teams
Import-Module MicrosoftTeams
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential
```

After connecting to Teams PowerShell module, run the next command to create a new dial plan:

```
New-CsTenantDialPlan -Identity Blouc-CA-Tracy -Description "Dial Plan
for CA Tracy" -NormalizationRules <pslistmodifier> -ExternalAccessPrefix
9 -SimpleName "Dial-Plan-for-CA-Tracy"
```

If you want to edit existing dial plan settings, then use this PowerShell command:

```
Set-CsTenantDialPlan -Identity Bloguc-CA-Tracy -NormalizationRules
<pslistmodifier> -ExternalAccessPrefix 9 -SimpleName "Dial-Plan-for-
CA-Tracy"
```

To assign users to a dial plan, use this PowerShell command:

```
Grant-CsTenantDialPlan -Identity bilag@bloguc.com -PolicyName
Bloguc-CA-Tracy
```

If you want to delete a dial plan, then use this PowerShell command:

```
Remove-CsTenantDialPlan -Identity Bloguc-CA-Tracy -force
```

Sometimes you need to see what dial plan is assigned to a user. To do that, use the next PowerShell command:

```
Get-CsEffectiveTenantDialPlan -Identity bilag@bloguc.com
```

Another important task that you can achieve through PowerShell commands is to test the effective tenant dial plan using a dialed number and user account. To do so, use this PowerShell command:

```
Test-CsEffectiveTenantDialPlan -DialedNumber 14255550199 -Identity bilag@bloguc.com
```

If you want to add a normalization rule to the existing tenant dial plan, use the following PowerShell command:

```
$nr1=New-CsVoiceNormalizationRule -Parent Global -Description 'Organization extension dialing' -Pattern '^(\d{3})$' -Translation '+140855551$1' -Name NR1 -IsInternalExtension $false -InMemory  
Set-CsTenantDialPlan -Identity Bloguc-CA-Tracy -NormalizationRules @{add=$nr1}
```

If you want to remove a normalization rule from the existing tenant dial plan, use this PowerShell command:

```
$nr1=New-CsVoiceNormalizationRule -Parent Global/NR1 -InMemory  
Set-CsTenantDialPlan -Identity Bloguc-CA-Tracy -NormalizationRules @{remove=$nr1}
```

To find all users who have been granted the Bloguc-CA-Tracy tenant dial plan, use this command:

```
Get-CsOnlineUser | Where-Object {$_.TenantDialPlan -eq "Bloguc-CA-Tracy"}
```

Refer to the PowerShell reference documents for more information: <https://learn.microsoft.com/en-US/microsoftteams/create-and-manage-dial-plans#using-powershell>.

Emergency Policies

Emergency calling policies are used to control how users in your organization can use dynamic emergency calling features. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies for those people within your organization.

Emergency Calling Policies

As a Teams admin, you can manage emergency calling policies by going to the Teams admin center and then navigating to Voice. You can then use Emergency Policies and Calling Policies in the Microsoft Teams admin center or Windows PowerShell.

For users, you can use the Global (Org-wide default) policy or create and assign custom policies. Users will automatically get the Global policy unless you create and assign a custom policy. Keep in mind that 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.

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 that is assigned to the network site overrides the policy that is assigned to the user.

Using the Microsoft Teams Admin Center

Follow these steps:

1. Log in to the Teams admin center, and then navigate to Voice. Select Emergency Policies, and then click the “Calling policies” tab and click +Add.
2. On the next screen, enter a name and description for the policy and then set how you want to notify people in your organization, typically the security desk, when an emergency call is made. To do this, under Notification Mode, select one of the following options:
 - *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*: A Teams chat message is sent to the users and groups that you specify, and they can listen as well as participate in the conversation between the caller and the PSAP operator.

In the example shown in Figure 2-101, “Conference in but are muted” is selected.

3. Enter the dial-out number for notifications and then 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 notification can be sent to email addresses of users, distribution groups, and security groups. A maximum of 50 users can be notified. Figure 2-101 shows an example emergency calling policy.

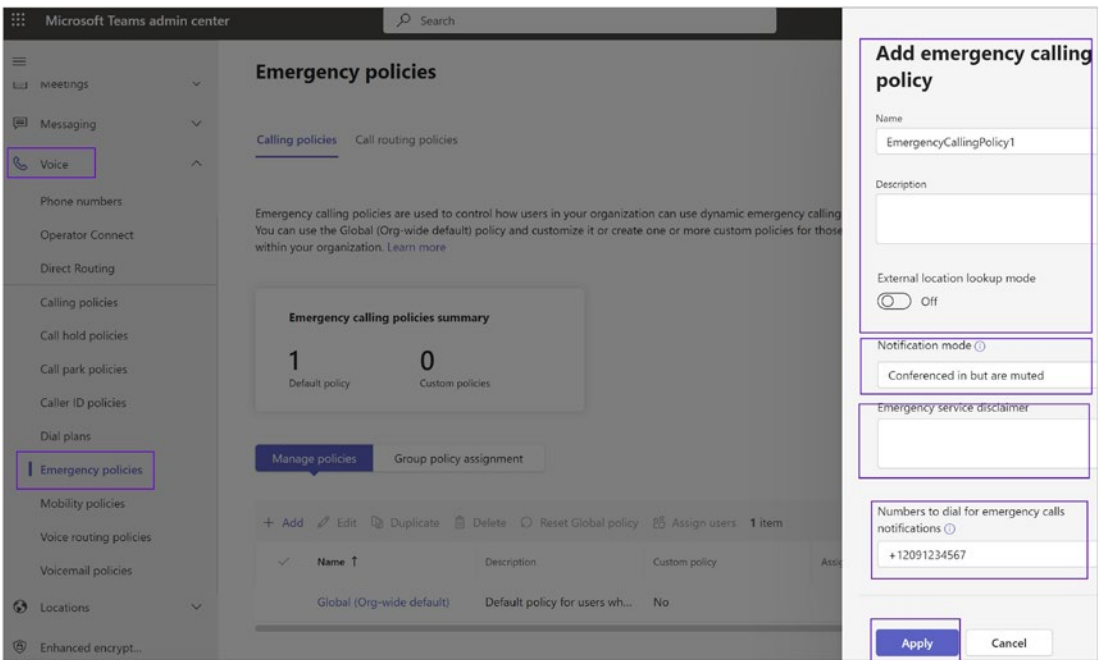


Figure 2-101. Emergency calling policy

4. Once all settings are complete, click Apply.

You can also set the emergency calling policy using PowerShell, using this command:

```
New-CsTeamsEmergencyCallingPolicy -Identity EmergencyCallingPolicy1  
-Description "EMS Group HQ" -NotificationGroup "bilag@bloguc.com"  
-NotificationDialOutNumber "1234567890" -NotificationMode NotificationOnly  
-ExternalLocationLookupMode $true
```

Assigning a Custom Emergency Calling Policy to Users in a Group

After creating an emergency calling policy, the next thing you need to do is assign a custom emergency calling policy to multiple users that you've already identified using the Teams admin center or PowerShell.

Assigning an Emergency Calling Policy Using Teams Admin Center

Log in to the Teams admin center and navigate to Users. Select the user and then click Policies. Under Assigned Policies, click Edit. Under Emergency Calling Policy, select the newly created policy. Finally, click Save to commit the changes. In our example, the policy name is EmergencyCallingPolicy1.

Note You can assign an emergency calling policy to users through the Emergency Calling Policy page itself by clicking Manage User.

Tip As a best practice, assign an emergency call routing policy to users as well as to a network site to cover those who are not at the network site location.

Assigning Emergency Calling Policy Using PowerShell

For example, you might want to assign a policy to all users in a security group. You can do this by connecting to the Azure AD PowerShell for Graph module and the Teams PowerShell module. In this example, we assign a policy called Operations Emergency Calling Policy to all users in the Bloguc Security group.

```
Group = Get-AzureADGroup -SearchString "Bloguc Security Group"
$members = Get-AzureADGroupMember -ObjectId $group.ObjectId -All $true |
Where-Object {$_.ObjectType -eq "User"}
$members | ForEach-Object { Grant-CsTeamsChannelsPolicy -PolicyName
"EmergencyCallingPolicy1" -Identity $_.UserPrincipalName}
```

Note Depending on the number of members in the group, this command might take several minutes to execute.

Assigning an Emergency Calling Policy to the Network Site

This is an important requirement. To assign an emergency calling policy to the network, run the following PowerShell command, which uses the `Set-CsTenantNetworkSite` command to assign an emergency calling policy to a network site:

```
Set-CsTenantNetworkSite -identity "site1" -EmergencyCallingPolicy
"Bloguc Emergency Calling Policy 1"
```

Emergency Call Routing Policies

After creating an emergency calling policy, you next need to create emergency call routing policies. These policies are used to set up emergency numbers and then specify how those emergency calls are routed. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies for those users within your organization.

However, before creating an emergency call routing policy, you must understand why you are creating these policies. For example, if you have deployed Phone System Direct Routing in your organization, you can use emergency call routing policies in Microsoft Teams to set up emergency numbers and specify how emergency calls are routed. An emergency call routing policy determines whether enhanced emergency services are enabled for users who are assigned the policy, the numbers used to call emergency services (e.g., the 911 calling service in the United States), and how calls to emergency services are routed. Out of the box, the Global (Org-wide default) policy is available, or you can create and assign custom policies. Users will automatically get the Global policy unless you create and assign a custom policy.

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

Creating and Managing Emergency Call Routing Policy

Admins can create an emergency call routing policy using the Teams admin center as well as PowerShell. To create an emergency call routing policy using the Teams admin center, follow these steps:

1. Log in to the Teams admin center and navigate to Voice. Select Emergency Policies, and then click the Call Routing Policies tab. Click +Add.
2. On the Emergency Call Routing Policy page, enter a meaningful name and description for the policy.
3. To enable enhanced emergency services, turn on the Enhanced Emergency Services option. When enhanced emergency services are enabled, Teams retrieves the policy and location information from the service and includes that information as part of the emergency call. Figure 2-102 shows the enhanced emergency services enabled.

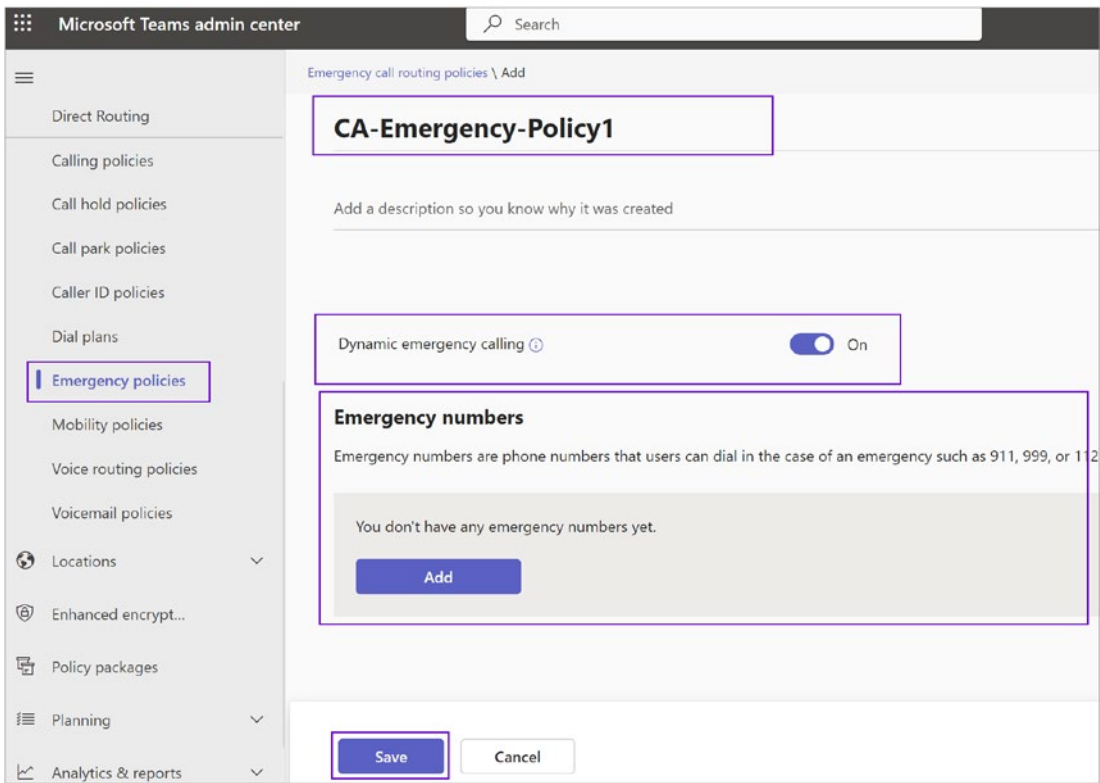


Figure 2-102. Emergency call routing policy

4. The next thing you need to do to identify one or more emergency numbers. To do this, under Emergency Numbers, do the following:
 - a. *Emergency dial string*: Enter the emergency dial string. This dial string indicates that a call is an emergency call. Refer to Figure 2-103, which shows 911 as the dial string.
 - b. *Emergency dial mask*: For each emergency number, you can specify zero or more emergency dial masks. A dial mask is the number that you want to translate into the value of the emergency dial string. This allows for alternate emergency numbers to be dialed and still have the call reach emergency services. For example, you can add 112 as the emergency dial mask, which is the emergency service number for most of

Europe, and you can add 911 as the emergency dial string. A Teams user from Europe who is visiting might not know that 911 is the emergency number in the United States, and when they dial 112, the call will be made to 911. To define multiple dial masks, separate each value by a semicolon (e.g., 112;212). See Figure 2-103.

- c. *PSTN usage record*: Select the PSTN usage record. The PSTN usage determines which route is used to route emergency calls from users who are authorized to use them. The route associated with this usage should point to a Session Initiation Protocol (SIP) trunk dedicated to emergency calls or to an Emergency Location Identification Number (ELIN) gateway that routes emergency calls to the nearest PSAP. See Figure 2-103.

CA-Emergency-Policy1

Add a description so you know why it was created

Dynamic emergency calling On

Emergency numbers

Emergency numbers are phone numbers that users can dial in the case of an emergency such as 911, 999, or 112.

Emergency dial string ⓘ	Emergency dial mask ⓘ	PSTN usage record
911	112;212	Unrestricted ×

+ Add

Save Cancel

Figure 2-103. *Emergency numbers*

5. Once you are finished adding all emergency numbers, click Save. Remember, Figure 2-103 shows an example, not a real policy that you can follow. You as an admin need to come up with an emergency string and dial mask before creating the emergency number.

Emergency Call Routing Policy to Users Using the Teams Admin Center and PowerShell

To assign an emergency routing policy to users using the Teams admin center, follow this procedure:

1. Log in to the Teams admin center, and then navigate to Users. Select the user and then click Policies.
2. Under Assigned Policies, click Edit.
3. Under Emergency Call Routing Policy, select the policy you want to assign (e.g., CA-Emergency-Policy1), and then click Save.

Note You can assign an emergency calling policy to users using the Emergency Calling Policy page itself by clicking Manage User.

Assigning an Emergency Calling Policy Using PowerShell

Before running the PowerShell command, you first connect to the Azure AD PowerShell for Graph module and the Teams PowerShell Online module by following the steps in “Connect to All Office 365 Services in a Single Windows PowerShell Window” (<https://bloguc.com/connect-to-multiple-office-365-services-in-a-one-powershell-window/>).

```
$group = Get-AzureADGroup -SearchString "Bloguc IT"
```

Get the members of the specified group (Bloguc IT).

```
$members = Get-AzureADGroupMember -ObjectId $group.ObjectId -All $true |  
Where-Object {$_.ObjectType -eq "User"}
```


Then assign all users in the group to a particular Teams policy. In this example, it's `EmergencyCallRoutingPolicy1`. First connect the Teams PowerShell module.

```
# When using Teams PowerShell Module
Import-Module MicrosoftTeams
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential
# Then run the command.
$members | ForEach-Object { Grant-CsTeamsEmergencyCallRoutingPolicy
-PolicyName "CA-Emergency-Policy1" -Identity $_.UserPrincipalName}
```

Note Depending on the number of members in the group, this command could take several minutes to execute.

Assigning a Custom Emergency Call Routing Policy to a Network Site

It is important to assign an emergency call routing policy to the network site using the `Set-CsTenantNetworkSite` command to use a network site or subnet with the same policy. This example shows how to assign a policy called `EmergencyCallRoutingPolicy1` to the `BlogucSite1` site.

```
Set-CsTenantNetworkSite -Identity "BlogucSite1" -EmergencyCallRoutingPolicy
"CA-Emergency-Policy1"
```

Mobility Policies

Mobility policies control the Teams Phone Mobile features that are available to users in Teams. You can use the Global (Org-wide default) policy or create one or more custom mobility policies for people in your organization. Figure 2-104 shows the Teams mobility policy. You can use a default global policy or create a new custom policy.

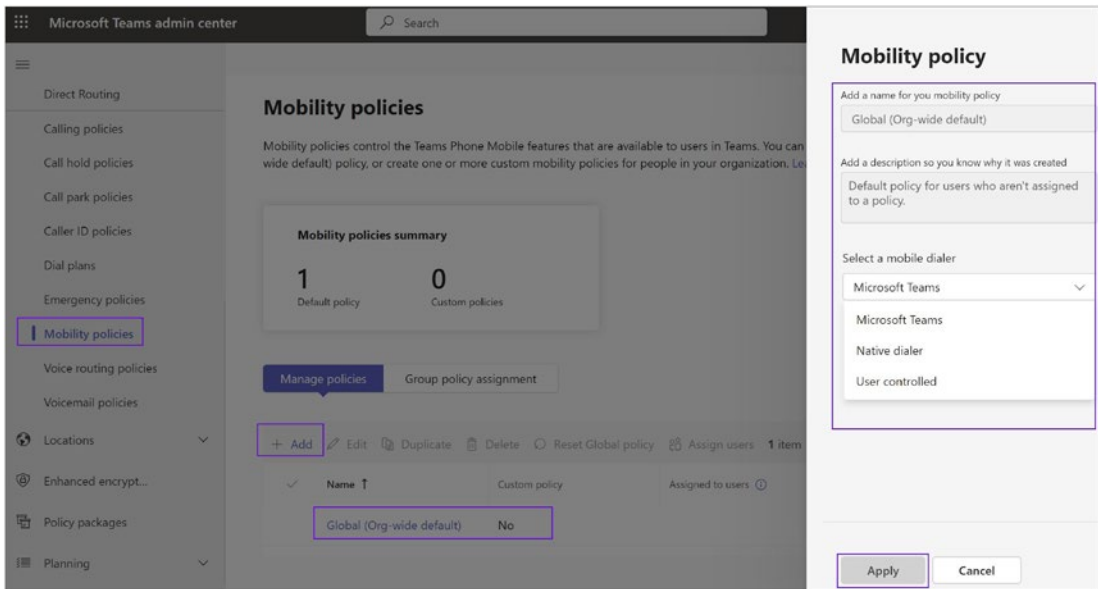


Figure 2-104. Teams mobility policy

Voice Routing Policies

Voice routing policies in Microsoft Teams determine how calls are routed. These policies specify a set of Public Switched Telephone Network (PSTN) usages that define which voice routes are assigned to users who are homed online.

Setting up a voice routing policy involves creating and assigning PSTN usages, creating voice routes, and then creating the policy itself.

To create and manage Teams Voice routing policy in the Teams admin center, you would do the following:

1. Log in to the Teams admin center.
2. Navigate to Voice, click Voice Routing Policies, and then click +Add to create a new voice routing policy. You can use a global policy; however, creating a new custom policy for each calling scenarios is recommended.

- On the next page, give a meaningful name and description and then click “Add PSTN usage records.” On the next page, click +Add to create a new PSTN usage record. Give a meaningful name, check the newly created PSTN record, and click “Save and apply.” For example, use “CA-National-Usage.” Figure 2-105 shows the voice route policy and PSTN usage creation settings.

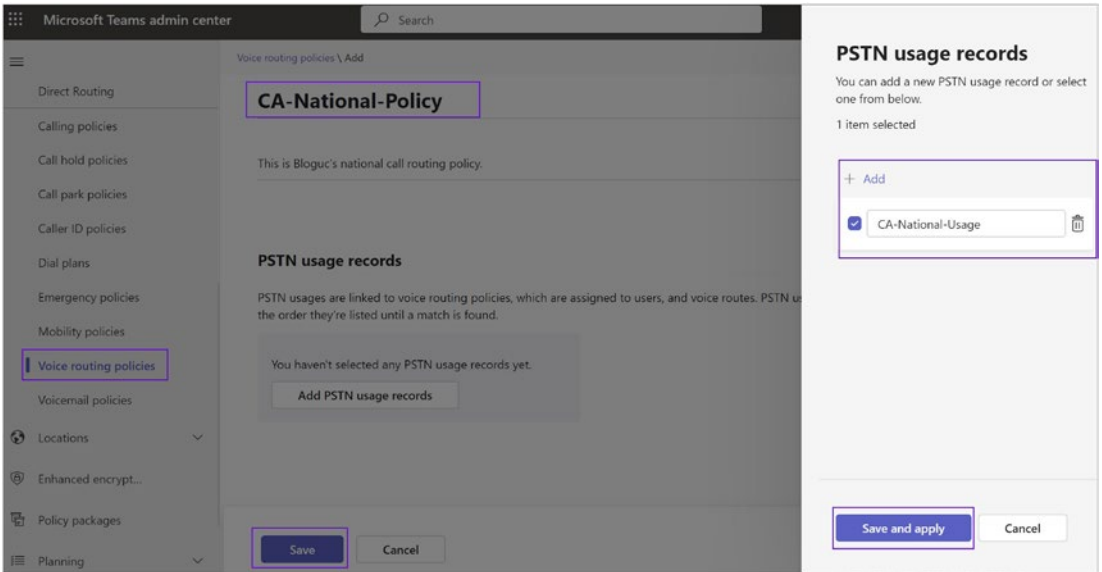


Figure 2-105. Teams voice routing policy

- The next thing you need to create is a voice route. The voice route option is available in the Teams admin center; click Voice ► Direct Routing ► Voice route.
- Then click +Add to create new route. Figure 2-106 shows the voice route creation; you need to give a meaningful name, add the SBC, and then select the appropriate PSTN Usage. For example, Figure 2-106 shows CA-National-Usage.

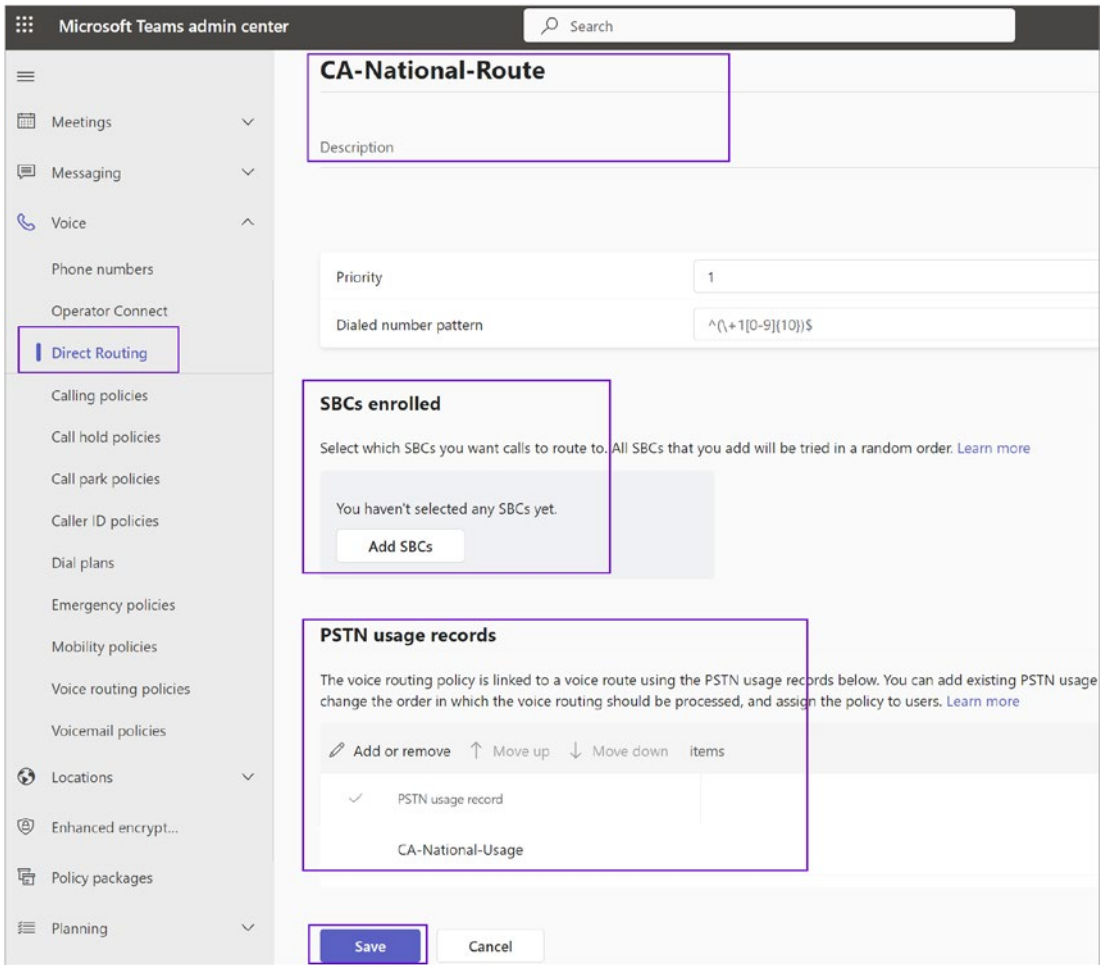


Figure 2-106. Teams voice routing policy

Creating Voice Routing Policies Using PowerShell

Here's how to use PowerShell.

Creating PSTN Usages

PSTN usages are labels that you assign to voice routes. They don't describe or define a route but are just a way to group routes. To create a PSTN usage, you use the `New-CsPstnUsage` cmdlet.

```
# When using Teams PowerShell Module
Import-Module MicrosoftTeams
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential
```

Here's an example:

```
New-CsPstnUsage -Identity Global -Usage "CA-National-Usage"
```

Creating Voice Routes

Voice routes contain instructions on how to route calls to specific numbers or number patterns. To create a voice route, you use the `New-CsVoiceRoute` cmdlet. Here's an example:

```
New-CsVoiceRoute -Identity "CA-National-Route" -NumberPattern
"^+\d{7}$" -PstnUsages @{"Add="CA-National-Route"} -PstnGatewayList
@{"Add="sbc1.bloguc.com"}
```

This command creates a new voice route that applies to numbers that match the specified pattern and sends them through the specified gateway. The `PstnUsages` parameter associates this route with the previously created PSTN usage.

Creating Voice Routing Policies

Voice routing policies tie PSTN usages to users. To create a voice routing policy, you use the `New-CsVoiceRoutingPolicy` cmdlet. Here's an example:

```
New-CsVoiceRoutingPolicy -Identity "CA-National-Policy" -PstnUsages
@{"Add="NationalRoute"}
```

This command creates a new voice routing policy and assigns it the `LocalRoute` PSTN usage.

Assigning Voice Routing Policies to Users

After creating the voice routing policy, you can assign it to users. Here's an example:

```
Grant-CsVoiceRoutingPolicy -Identity "bilag@bloguc.com" -PolicyName  
"NationalPolicy"
```

This command assigns the LocalPolicy voice routing policy to the user with the email address bilag@bloguc.com.

It's important to note that these are just basic examples. Real-world routing scenarios can be much more complex and might involve multiple usages, routes, and policies. Always plan your configuration carefully to ensure it meets your specific needs.

Remember that changes in PowerShell might take up to 15 minutes or more than that to propagate through Microsoft Teams.

Voicemail Policies

Voicemail policies control the available features for the voicemail service in Teams. You can use the Global (Org-wide default) policy and customize it or create custom voicemail policies for users in your organization. Figure 2-107 shows the voicemail policy settings including that users can edit call answering rules, maximum voicemail recording length, primary and secondary prompt language, voicemail transcription, translation for transcription, etc.

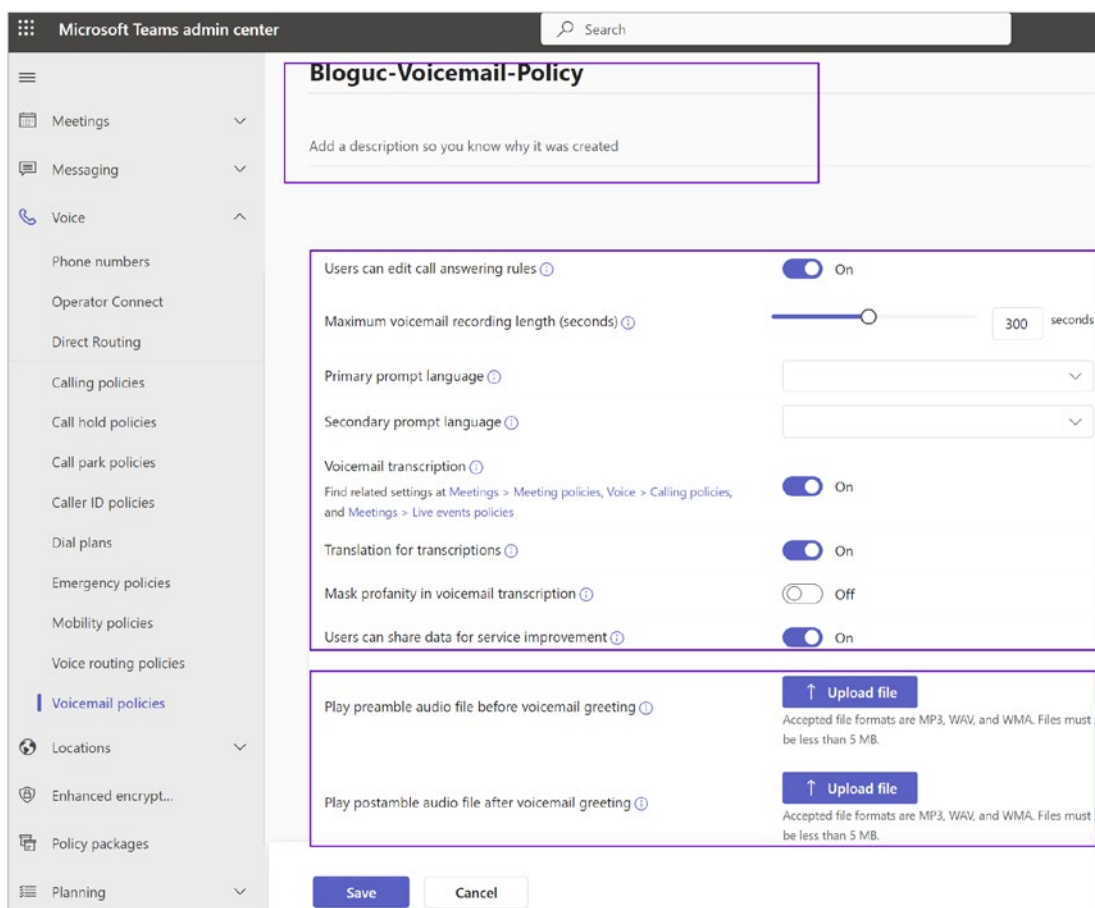


Figure 2-107. Teams voicemail policy

Admin Center: Locations Tab

In the Teams admin center, when you navigate locations, you will see three different options. Reporting labels is a way to upload your existing network's IP subnets with their physical office addresses to identify the site correctly in Teams reports and the Call Quality dashboard. Emergency addresses allows you to update physical office addresses that can be used for emergency services like Enhanced 911. Network topology itself offers a way to update network details including central and branch office designations with network site subnets and bandwidth details. Read each option carefully to understand Teams networking.

Emergency Addresses

An emergency location is a physical street address for your organization. To specify buildings, floors, or offices at a location, you can add places. Updating emergency addresses is critical because the emergency services such as 911 service are dependent on the emergency addresses updated in the Teams admin center. You as a Teams administrator must understand the emergency address update process, including how to update addresses, validation, formatting, and how emergency calls are routed to the public safety answering point (PSAP).

Emergency locations contain a physical address and, if needed, a specific indicator, like a building, floor, cubical or office, that is used to help locate a person in your organization if that user calls emergency services. You can create one or more addresses, depending on the number of physical locations you have in your organization. Basically, an emergency location could be referred to as a civic address, street address, or physical address. It is the street or civic address of a place of business for your organization that is used to route emergency calls to the appropriate dispatch authorities and to assist in locating the emergency caller. If your organization has multiple physical locations, you will need to add more than one emergency location.

After updating physical location addresses, your next task is to validate the emergency addresses that are added, making sure they are legitimate and correctly formatted for emergency response services. It is possible to add and save an emergency location that is not validated, but only validated locations can be associated with a user. After an emergency location is validated and saved, you can assign it to a user. You can also modify an emergency location that is saved and validated.

When an emergency location is assigned to a user, you will assign a location ID that references the location. The location ID includes the referenced emergency address (the street or civic address). A default place is included with an emergency location for cases in which in-building specifiers are not needed.

When a Teams user dials an emergency number, how the call is routed to the serving PSAP varies by country or region. In some countries or regions, such as the United States and the United Kingdom, the calls are first screened to determine the current location of the user before connecting the call to the appropriate dispatch center. In other areas, calls are routed directly to the dispatch center serving the phone number associated with the emergency caller.

To add an emergency address, follow these steps:

1. First, list all emergency locations, meaning all the physical addresses of your organization offices.
2. Once you are ready to add emergency locations, log in to the Teams admin center and navigate to Locations ► Emergency Addresses. Click +Add and then type the name of your location. Select the country and then type the address starting with office number, road, city, state, and area code. The example in Figure 2-108 shows the Bloguc HQ office address.

Microsoft Teams admin center Search

Bloguc HQ Office

Country or region
United States

Street number: 537
Street name: South Tradition Street

City: Tracy
State: California
Zip code: 95391

Latitude: 37.77205
Longitude: -121.54237

Organization name: HQ
ELIN (optional): ELIN (optional)

Why can't I change this address?

Save Cancel

Figure 2-108. Updating emergency addresses

Microsoft made address searching easier by allowing you to select Correct when you type the address. Once you click Save, it will automatically validate the address. After an address is added, this window shows the address status. Figure 2-109 shows the Bloguc HQ office address and its validation status.

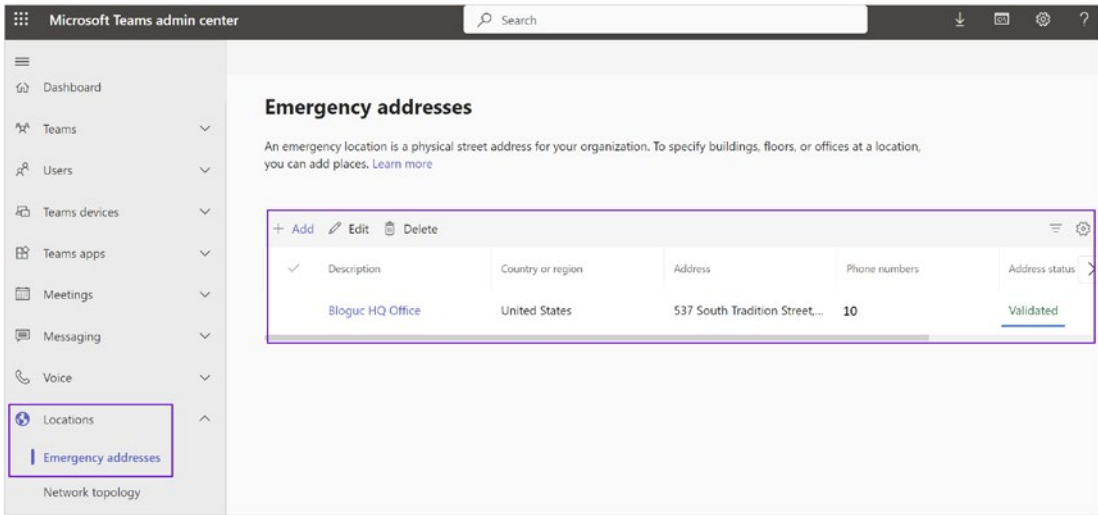


Figure 2-109. Emergency address added and validated

Note You can change the address information for a location only when the address is not validated. If the address was previously validated, you must delete the location and then create a new location.

Managing Emergency Location

As an admin, you can manage or modify an emergency location by changing, adding, or deleting location information, for example. To modify an emergency location, follow this procedure:

1. Log in to the Teams admin center and navigate to Location. On the Emergency Addresses page, select the location you want to change from the list, and then click Edit.

2. Make your changes.
3. Click Save.

To remove or delete an emergency location, visit the Emergency Addresses page in the Microsoft Teams admin center. Find and select the location you want to remove from the list of locations, and then click Delete.

Network Topology

You can use network topology to define the network regions, sites, and subnets that are used to determine the emergency call routing and calling policies that are to be used for a given location.

Inside the network topology you can add network sites and trusted IP addresses that are going to be used in call admission control, location-based routing, and so on. A network region contains a collection of network sites. You can add new network regions that can be used globally for all network sites. Follow this procedure to add a network site:

1. Log in to the Teams admin center and navigate to Location. On the Network Topology page, select Network Sites and then click Add.
2. Once the Add Network Site page opens, enter a network site name and description, and then set whether location based routing is enabled for this site. Select an emergency location, and finally click New to add the subnet. Figure 2-110 illustrates adding a network site.

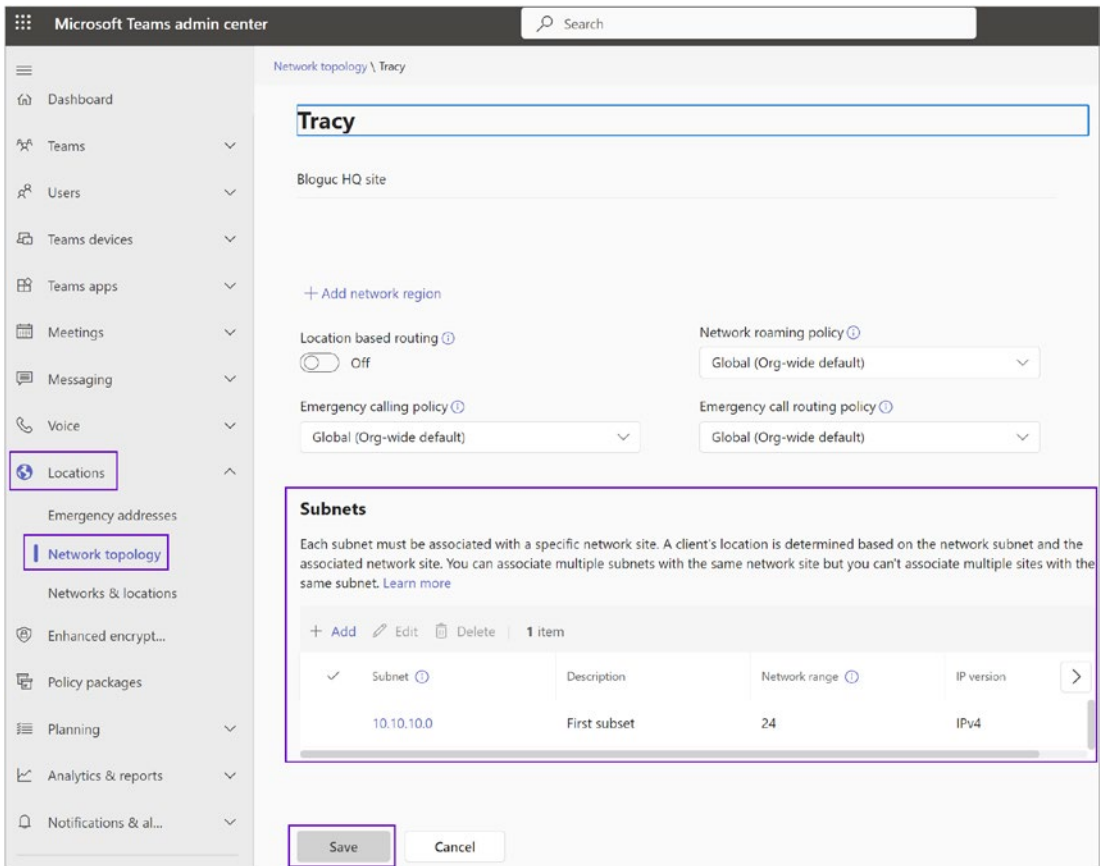


Figure 2-110. Network site

Click +New to add a new subnet with a subnet mask and IP version (see Figure 2-111).

Add subnet

You can divide your network into subnets. Dividing a network into subnets is useful for both security and performance reasons.

IP version
IPv4

IP address
10.10.10.0

Network range ⓘ
24

Description
First subnet

Apply Cancel

Figure 2-111. Adding a subnet

Adding Trusted Ips

Trusted external IP addresses are the external IP addresses of the enterprise network and are exempt from certain designated security options. To add trusted IP addresses on the Network Topology page, you can select Trusted IPs and then click Add. Enter the IP version, IP address, network range, and description, as shown in Figure 2-112. Trusted IP addresses are required to implement a location-based routing (LBR) service, as LBR checks to discover the internal subnet where the user's endpoint is located. If the user's external IP address doesn't match any IP address defined in the trusted IP address list, the endpoint is categorized as being at an unfamiliar location, and any PSTN calls to or from a user who is enabled for location-based routing are blocked.

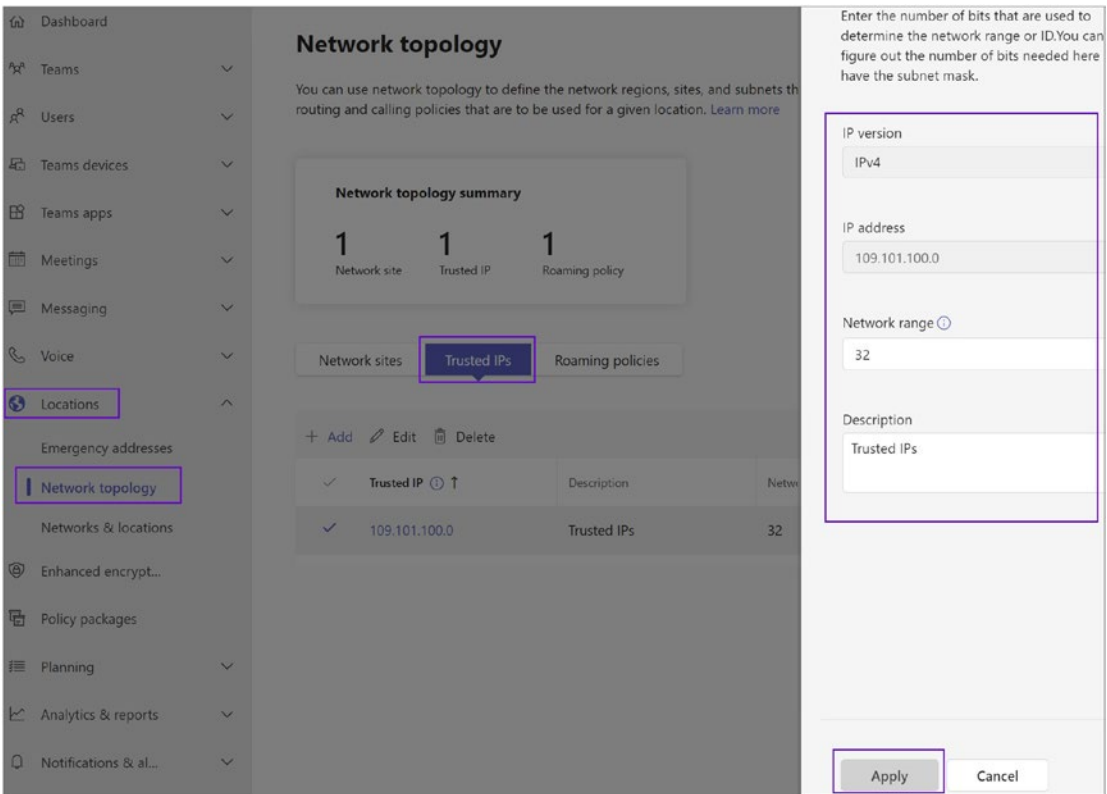


Figure 2-112. Adding a trusted IP

Roaming Policies

You can manage video and media settings with the network roaming policy.

In addition to managing video and media settings with meeting policies, you can now dynamically control the use of the following attributes used by the Microsoft Teams client by using the TeamsNetworkRoamingPolicy: IP Video and Media bit rate settings. Figure 2-113 shows the roaming policy with the “Media bit rate (Kbs)” config option.

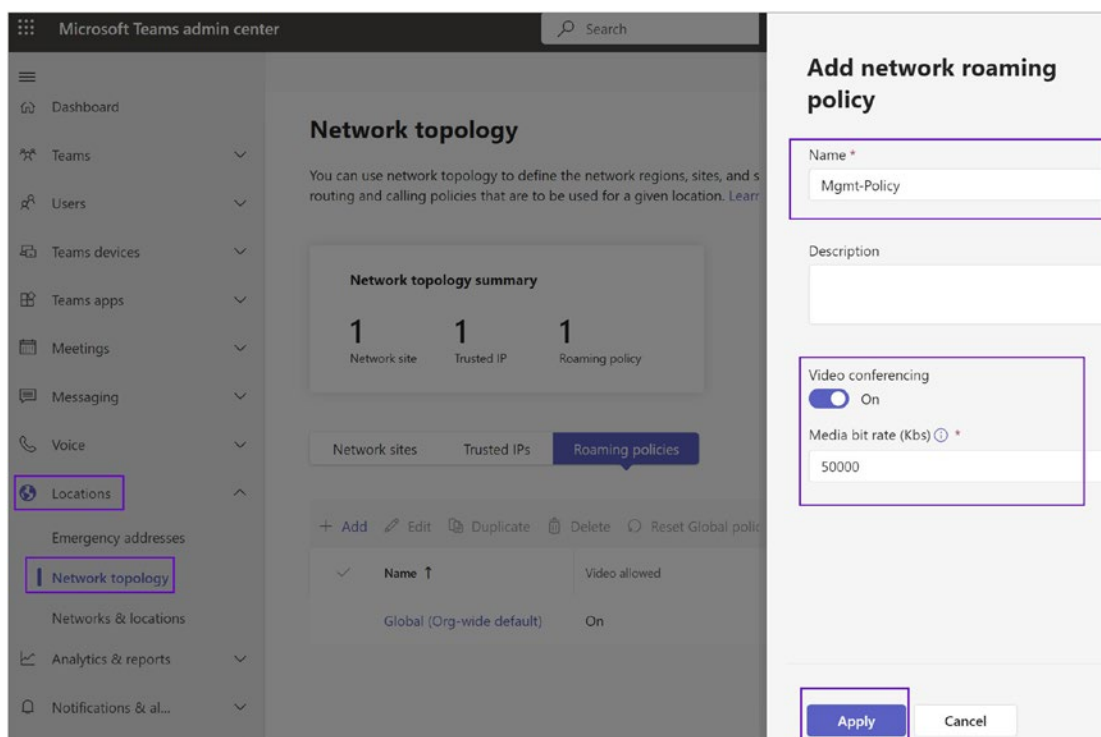


Figure 2-113. Adding a trusted IP address

Networks and Locations

In the Microsoft Teams admin center, under Networks and Locations, you can view and manage information about your organization's network. This includes subnets, Wi-Fi access points, switches, and ports, which together help the Teams client to obtain emergency addresses from the locations associated with different network identifiers. For a client to obtain a location, you as Teams admin must fill the location information server (LIS) with network identifiers (subnets, WAPs, switches, ports) and emergency locations. You can do this in the Microsoft Teams admin center or by using PowerShell.

Here's a breakdown of each component:

Subnets: A network subnet defines a segment of the IP network that contains the addresses of one or more endpoints. Each subnet must be associated with an emergency location, and the subnet ID must match the client network.

Wi-Fi access points: A wireless access point (WAP), also referred to as an access point (AP), is a networking device that allows other Wi-Fi devices such as PCs, laptops, and mobile phones to connect to a wired network. Each WAP is assigned a Basic Service Set Identifier (BSSID) used for grouping wireless network devices that operate with the same network parameters.

Switches: A network switch is a device that connects multiple local area network (LAN) devices, such as desktops running the Teams app, using Ethernet connections. The devices use this connection to receive and transfer data to each other. Each network switch is stamped with a chassis ID, which identifies the switch on the network.

Ports: A network port is a physical Ethernet connection that connects multiple local area network (LAN) devices such as a desktop computer that is running the Teams app. For each port, you need to enter the chassis ID of the network switch that connects the port to a switch in Teams.

Admin Center: Enhanced Encryption Policies

Enhanced encryption policies are used to control if users in your organization can use enhanced encryption settings in Teams. You can use the Global (Org-wide default) policy, or you can create one or more custom policies and then assign them to users. As part of the enhanced encryption, you as an admin can create a custom policy and enable one-on-one Teams calls that are end-to-end encrypted if both participants turn on this setting. Some features won't be available, including recording and transcription. Chat messages are secured by Teams data encryption. End-to-end encryption is part of Team premium license. Figure 2-114 shows three default policies and an option to create custom policies.

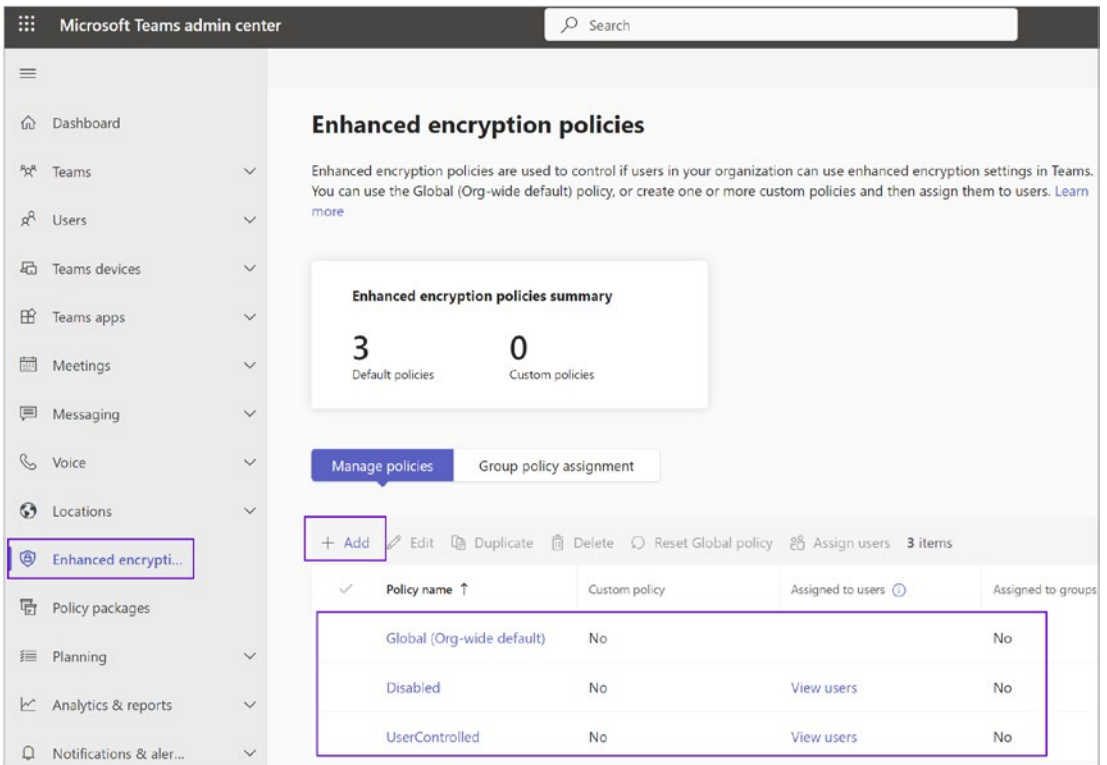


Figure 2-114. Enhanced encryption policy

Admin Center: Policy Packages

A policy package is a collection of predefined policies and settings that can be customized and applied to a group of users that have similar roles within your organization. You'll need Teams Premium or an Advanced Communications license to add, edit, duplicate, or manage users for custom policy packages. Figure 2-115 shows 14 policy packages that are available by default. However, you cannot create a custom policy package without a Teams Premium license. You can use an existing policy package and group policy assignment option.

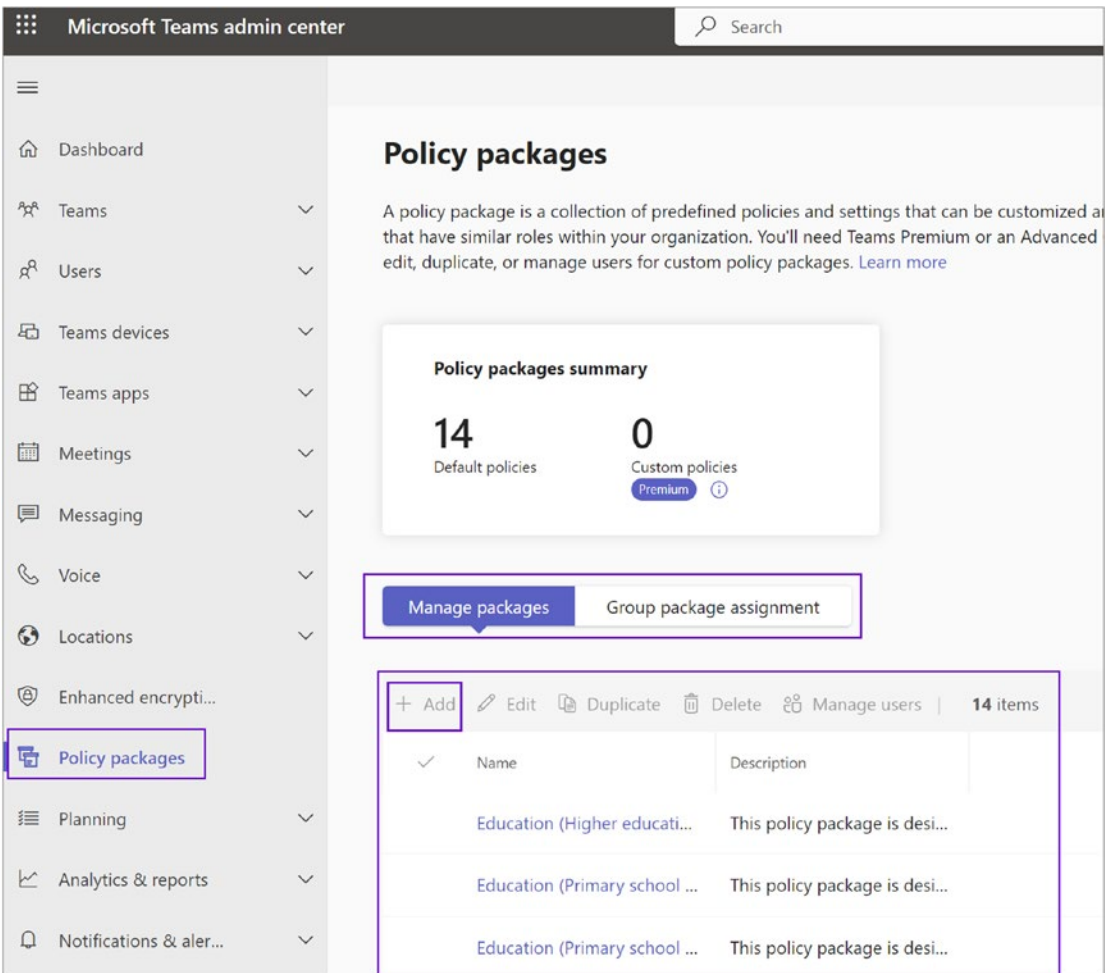


Figure 2-115. Policy packages

Admin Center: Planning

In the Microsoft Teams admin center, the Planning tab provides tools and resources to help you plan for deploying Teams in your organization. As a Teams admin, you need to ensure your existing environment is ready for handling the Teams workload and added media traffic before deploying Microsoft Teams in a production environment. You should check that the existing network infrastructure of an organization will meet the requirements needed for Teams collaboration and real-time communication.

In this discussion, we'll explore how to leverage Teams Advisor for optimal Teams deployment planning. It's crucial to guarantee sufficient bandwidth, complete access

to necessary IP addresses, and the appropriate configuration of ports when deploying Microsoft Teams within your network. Furthermore, fulfilling the performance demands for real-time media is a pivotal aspect of this planning process.

Advisor for Teams

Teams Advisor is a tool that helps you roll out Teams by providing a recommended deployment plan based on your organization's needs. The Teams Advisor generates a plan with a list of tasks that guide you through deploying Teams. It focuses on different workloads, including chat, teams, channels, apps, meetings, conferencing, and PSTN calling.

For example, if you're planning to deploy Teams for the first time in your organization, you could use the Teams Advisor to create a deployment plan. The Advisor would provide a list of tasks and step-by-step instructions to help you prepare your organization, configure settings, and train your users.

What Advisor for Teams Can Do

There are multiple things that Advisor for Teams can provide, and here we cover a few of them. Customers can select what workload they want to roll out and who they are rolling it out with. A tenant readiness assessment is provided based on common friction points that FastTrack has helped customers solve. Teams is created with the project team and populated with success resources to get started quickly.

Using Advisor for Teams

To use Advisor for Teams, you need to log in to the Teams admin center and then select Planning. Select Advisor for Teams and then click Add to select a workload to roll out in your organization. If this is the first workload you roll out, start with chat, teams, channels, and apps. Based on your selection, if a service management team doesn't exist, a team will be created with a channel dedicated to that workload. Prepopulated success resources listed under Details will be added into the team. Should you need to add additional workloads, you can at any time once the team is created. Repeat the same process to add another workload as Meetings and Conferencing. After adding both workloads, you will see them under Deployment Team, as shown in Figure 2-116.

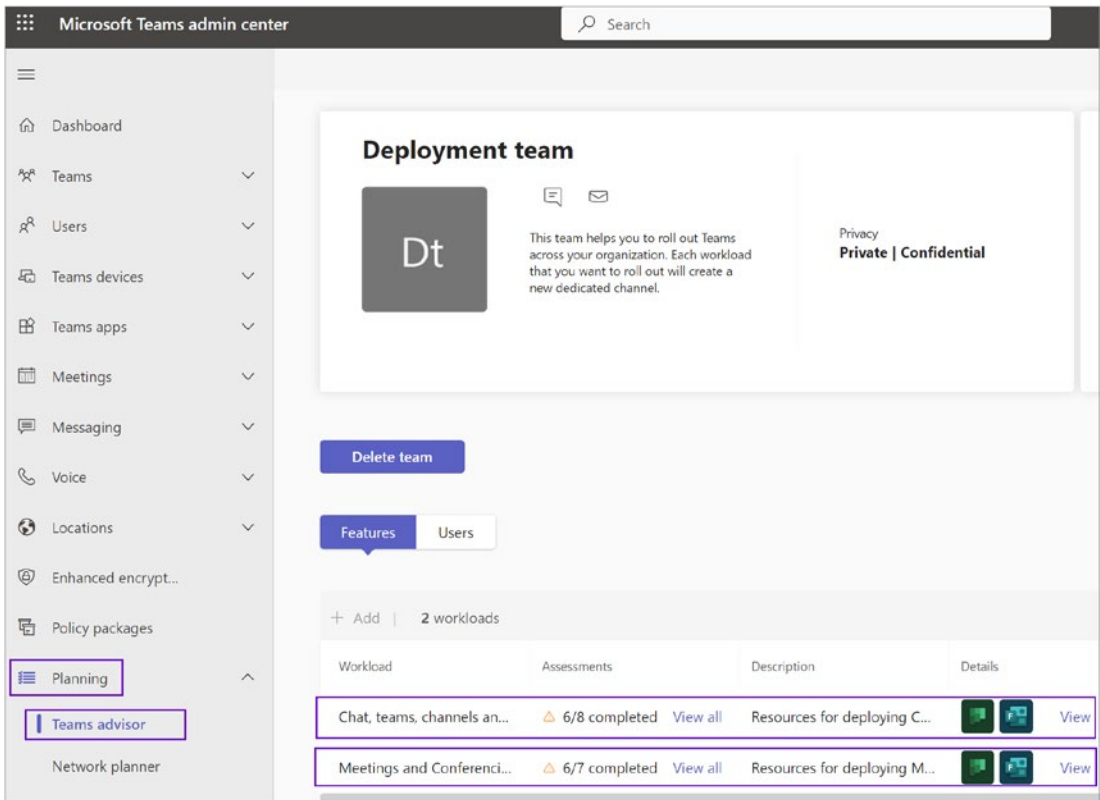


Figure 2-116. Two workloads

On the Users tab, you add users who can execute the deployment tasks.

Advisor for Teams has two core workloads covered. The first one includes chat, teams, channels, and apps; the second one is Meetings and Conferencing. Advisor for Teams runs the assessment and then highlights the areas that require more attention. As an example, Figure 2-117 shows two areas that need more attention: Office 365 Group Naming Standard Configured and Office 365 Group Expiration Configured. The rest of the tasks shown are completed.

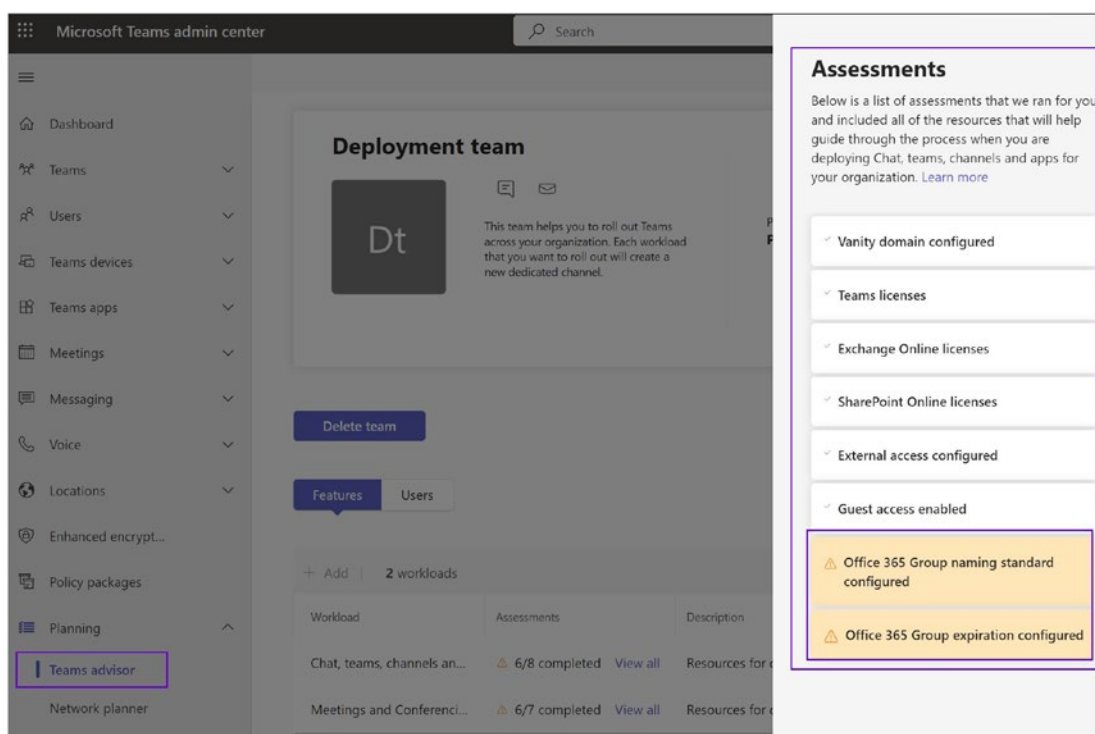


Figure 2-117. Advisor for Teams assessment

Advisor also gives recommended plans—basically step-by-step guidance—of how to best deploy this workload in Teams. This workload detail looks familiar, as it is actually coming from a planner. This is the plan that Microsoft Teams creates for the deployment team with all the details about how to deploy these workloads in Microsoft Teams.

On the Advisor for Teams main screen, you can see the deployment status as well. Advisor for Teams can open in your Teams and shows both the channels. Clicking the individual channel and Planner tab, you can see all the tasks for that workload. Because it is a shared workspace for deployment Teams, all the members can update the tasks.

Before starting Teams deployment, you must add all the project team members who are going to execute deployment tasks. Adding a member is easy; you can open the deployment team in Teams and add multiple members who are going to execute tasks.

Network Planner

The Network Planner helps you calculate and manage network requirements for deploying and running Teams in your organization. You input information about your organization's network and the Teams features you plan to use, and the Network Planner uses this information to calculate network requirements.

For example, if you're planning to introduce Teams meetings and calling in your organization, you could use the Network Planner to estimate the network impact. You would input information about your offices, network connections, and anticipated usage, and the Network Planner would provide an estimate of the bandwidth you'll need to support Teams.

In both cases, these tools are intended to help you plan and manage your Teams deployment more effectively. They provide guidance and recommendations based on your specific needs and help you anticipate and address potential issues before they become problems. However, they're not a substitute for broader planning and management efforts, and they should be used in conjunction with other best practices for deploying and managing Teams.

Network Planner helps you to determine and organize network requirements for connecting people who use Teams across your organization in a few steps. By providing your networking details and Teams usage, you get calculations and the network requirements you need when deploying Teams and cloud voice across organizational physical locations.

Using Network Planner, an admin can create representations of the organization using sites and Microsoft-recommended personas (office workers, remote workers, and Teams room system devices) and then generate reports and calculate bandwidth requirements for Teams usage.

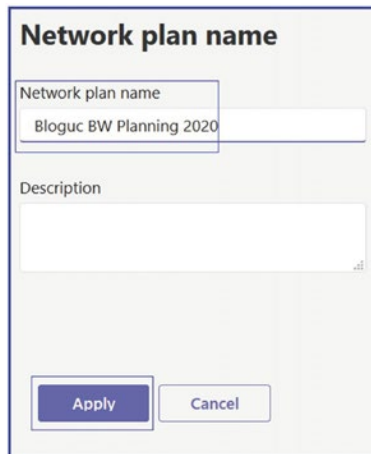
To use Network Planner, you must have global administrator, Teams admin, or Teams communication administrator role permission. You can access the Network Planner tool through the Microsoft Teams admin center. Select Planning and then Network Planner.

When you click Add, it will allow you to create a Network Planner name. By default, there will be three user personas, but you can add custom persons on the Network Planner page. Click the Users tab, and then on the Add Persona page, provide the persona name and description. In the Permissions section, select from the following services: Audio, Video, Screen Sharing, File Sharing, Conference Audio, Conference Video, Conference Screen Sharing, and PSTN.

Building a Network Planner Plan

Network Planner helps you to determine and organize network requirements for connecting people who use Teams across your organization in a few steps. To build your network plan, follow these steps:

1. Log in to the Microsoft Teams admin center, navigate to Planning, and select Network Planner.
2. On the Network Planner page, under Network Plans, click Add, as shown in Figure 2-118.
3. On the Network Plan name page, enter the name for the network plan (e.g., Bloguc BW Planning 2020 in Figure 2-118) and an optional description, and click Apply.



The screenshot shows a form titled "Network plan name". It contains two text input fields. The first field is labeled "Network plan name" and contains the text "Bloguc BW Planning 2020". The second field is labeled "Description" and is currently empty. At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 2-118. Assigning a network plan name

4. The newly created network plan will appear in the Network Plans section. Select the plan you created. On the plan page, in the Network Sites section, select Add A Network Site. On the Add A Network Site page, enter the following information:
 - Name of the network site
 - Network site address
 - Network settings: IP address subnet and network range
 - Express route or WAN connection
 - Internet egress
 - Internet link capacity
 - PSTN egress (VoIP only or local)
 - An optional description
5. Once you enter all details, as shown in Figure 2-119, click Save to commit the changes.

Microsoft Teams admin center

+ Create an address

Network users ⓘ
100

Network settings

Subnet
10.10.10.0

Network range
28

+ Add more

ExpressRoute ⓘ
 Off

Connected to WAN ⓘ
 On

WAN link capacity
50 Mbps

WAN audio queue size
10 Mbps

WAN video queue size
10 Mbps

Internet egress ⓘ
Local

Internet link capacity ⓘ
30 Mbps

PSTN egress ⓘ
Use VoIP only

Save Cancel

Figure 2-119. Adding a network site and subnet

Creating a Report

After creating a plan, you run the report to see the required bandwidth for the number of users per site. To create a report based on your network plan, perform the following steps:

1. Log in to the Microsoft Teams admin center. Navigate to Planning and then select Network Planner.

2. On the Network Planner page, under Network Plans, select your network plan (for this example, Bloguc BW Planning 2020).
3. On the plan page, select Report, and then click Add Report. On the Add Report page, enter the report name, and in the Calculation section, choose the type of persona, such as Office Worker or Remote Worker, and the number of users for each persona.
4. Click Generate Report, as shown in Figure 2-120.

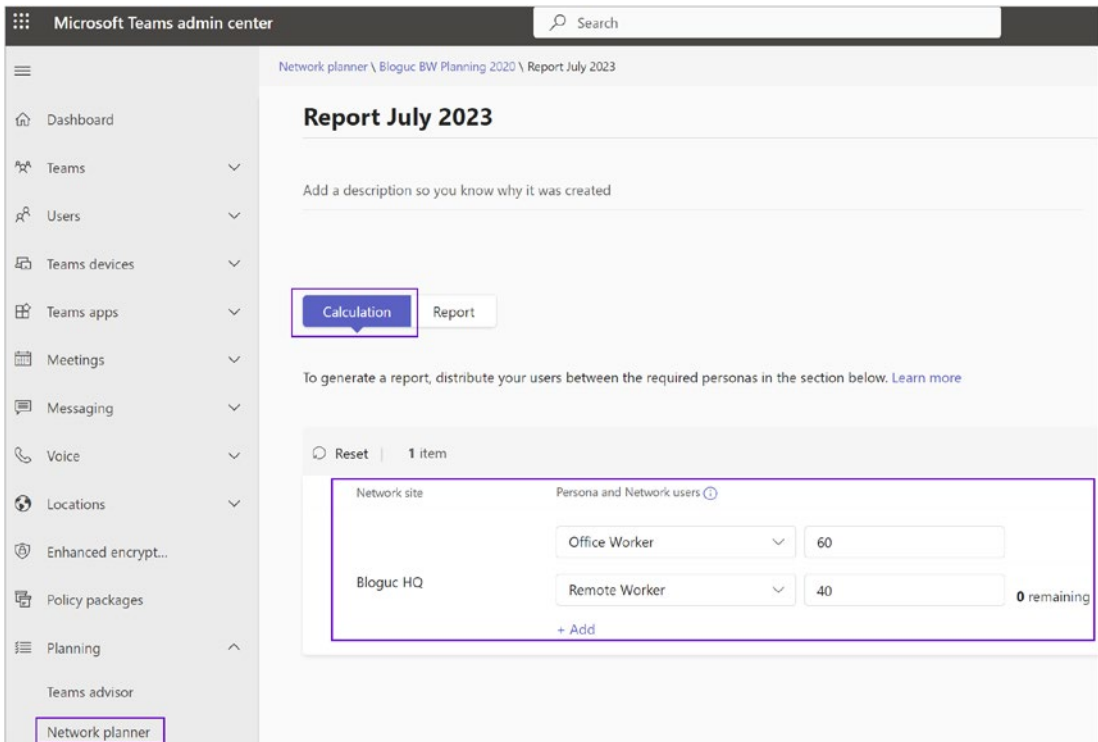


Figure 2-120. *Generating a report*

5. On the report page, review the report, including the type of service and required bandwidth for different services, such as audio, video, screenshare, Office 365 server traffic, and PSTN. Figure 2-121 shows the Network Planner report.

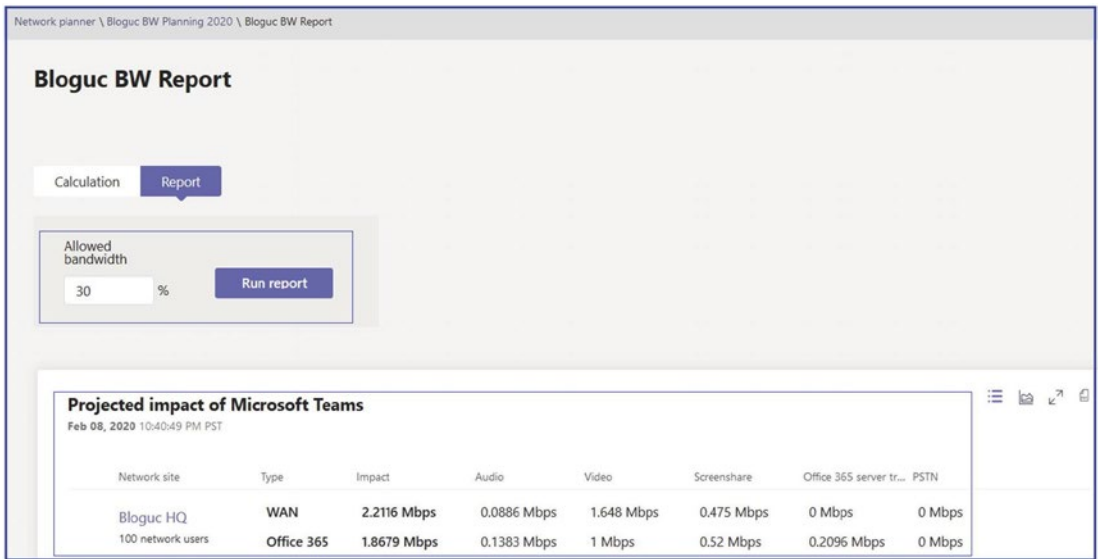


Figure 2-121. Network Planner report

Admin Center: Analytics and Reports

Teams reporting is important because it will improve the overall Teams deployment experience in your environment and how users will use Teams. Teams reporting provides user-level reporting and live event usage reports in the Teams admin center. The Analytics & Reports tab in the Teams admin center allows you to understand how your users are using Microsoft Teams, which features they are using, and their usage levels, which is important information for admins because it allows you to prioritize the training and readiness efforts.

To implement Microsoft Teams in the organization effectively, it is essential that you as a Teams admin generate reports that display usage activity in Teams, including the number of active users and channels. The Teams usage report helps you to understand users' adoption and verify how many users across your organization are using Teams to communicate and collaborate. Teams usage reports are available in the Microsoft Teams admin center. These reports provide usage information for teams, including the number of active users and channels, guests, and messages in each team.

Usage Reports

There are multiple types of reports available in the Teams admin center on the Analytics & Reports tab, and every report provides identical usage information. Brief details of each usage report are given next. These reports are all shown in Figure 2-122.

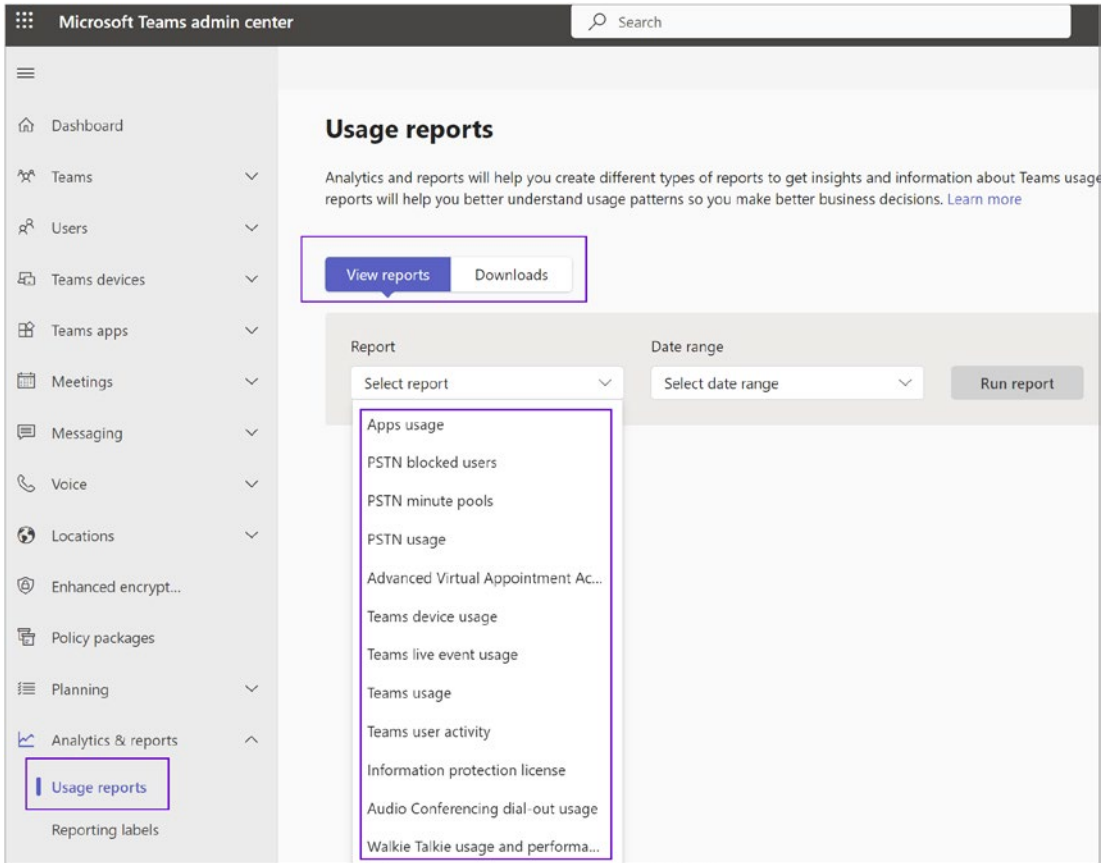


Figure 2-122. Available reports in the Teams admin center

- **Apps usage:** The Teams app usage report in the Microsoft Teams admin center provides you with insights about which apps users are using in Teams. You can gain insights into the app activity in your organization for different Microsoft (Viva learning, Shifts, etc.), third-party (Polly, Trello etc.), and line-of-business (LOB) Teams apps.

- *PSTN Blocked Users*: This report offers details of the display name, the phone number, the reason, the type of action, and the date and time of the action.
- *PSTN Minute Pools*: The Teams PSTN minute pools report in the Microsoft Teams admin center gives you an overview of audio conferencing and calling activity in your organization by showing you the number of minutes consumed during the current month. You can see a breakdown of activity including the license used for calls, total minutes available, used minutes, and license usage by location.
- *PSTN Usage*: This report offers usage information on Calling Plans as well as Direct Routing. The Teams PSTN and SMS usage report in the Microsoft Teams admin center gives you an overview of calling and audio conferencing activity in your organization. You can view detailed calling activity for Calling Plans if you use Microsoft as your telephony carrier and for Direct Routing if you use your own telephony carrier. The Calling Plans tab shows information including the number of minutes that users spent in inbound and outbound PSTN calls and the cost of these calls.
 - *Calling Plans*: This includes information on time stamp, username, phone number, call type, called to and called from, duration of the call, number type, charge, domestic or international call, conference ID, and capability (license).
 - *Direct Routing*: This includes information on time stamp, display name, SIP address, phone number, called to and called from, duration of the call, invite time, time of the call start, duration, failure time, number type, media bypass, SBC FQDN, event type, Azure region, final SIP code, final Microsoft subcode, final SIP phrase, and correlation ID.
- *Advanced Virtual Appointment*: The Advanced Virtual Appointments activity report in the Microsoft Teams admin center provides user activity information for advanced Virtual Appointments capabilities that are available with Teams Premium. To view the report, you must

be a Global admin, Teams admin, Global reader, or Report reader, and your organization must be using advanced Virtual Appointments capabilities.

- *Teams Device Usage:* This report gives information on whether users are using Windows, Mac, iOS, or Android devices to access the Teams app.
- *Teams device usage:* The Microsoft 365 Reports dashboard shows you the activity overview across the products in your organization. It enables you to drill in to individual product-level reports to give you more granular insight about the activities within each product. Check out the Reports overview topic. In the Microsoft Teams device usage report, you can gain insights into the types of devices on which the Microsoft Teams apps is being used in your organization.
- *Teams Live Event Usage:* This report provides information on total views of a live event; starting time; the status of the event; which users had a role as organizer, presenter, and producer; the recording setting; and the production type.
- *Teams Usage:* This report offers information about active users, active users in teams and channels, active channels, messages, privacy setting of teams, and guests in a team.
- *Teams User Activity:* This report provides information on one-to-one calls, messages that the user has posted in a team chat or in a private chat, and the last activity date of a user.
- *Audio Conferencing Dial-out report:* The Audio Conferencing dial-out usage report in the Teams admin center gives you an overview of usage and dollars spent for the audio conferencing dial-out service. This report allows admins to consume user-level data in terms of communication credits spent and dial-out minutes used. It will help admins determine the future communication credits needed going forward from any point in time.

- *Walkie Talkie Usage and Performance Report*: The Walkie Talkie usage and performance report in the Microsoft Teams admin center gives you an overview of Walkie Talkie activity in your organization. The report provides information such as the number of push-to-talk (PTT) transmissions made and received, channel activity, transmission duration, and device and participant details.

Use this report to gain insight into Walkie Talkie usage trends and performance in your organization. To access the report, you must be a Global admin, Teams admin, Global reader, or Report reader.

Accessing Teams Reports

Now that you have seen how important the information is that Teams reports provide, the logical question is how you access these reports. To access the Teams usage reports, you should have one of the following roles: Microsoft/Office 365 global admin, Teams Service admin, or Skype for Business admin. All of these reports are accessed via the Microsoft Teams admin center. Some of the most useful and accessed reports are covered next.

Reporting Labels

Reporting labels are used to give an IP subnet a name that links it to a physical location such as offices, buildings, or organizational sites within your organization. They are used by the Call Quality Dashboard or call analytics to make it easier to see the name of a place instead of just an IP subnet in reports. You can upload a text file (.csv or .tsv) that has a list of physical locations and their associated network subnets.

To upload the locations data, log in to the Teams admin center, then navigate to Analytics and Reports, and then select Reporting Labels. Next, click Upload, as shown in Figure 2-123.

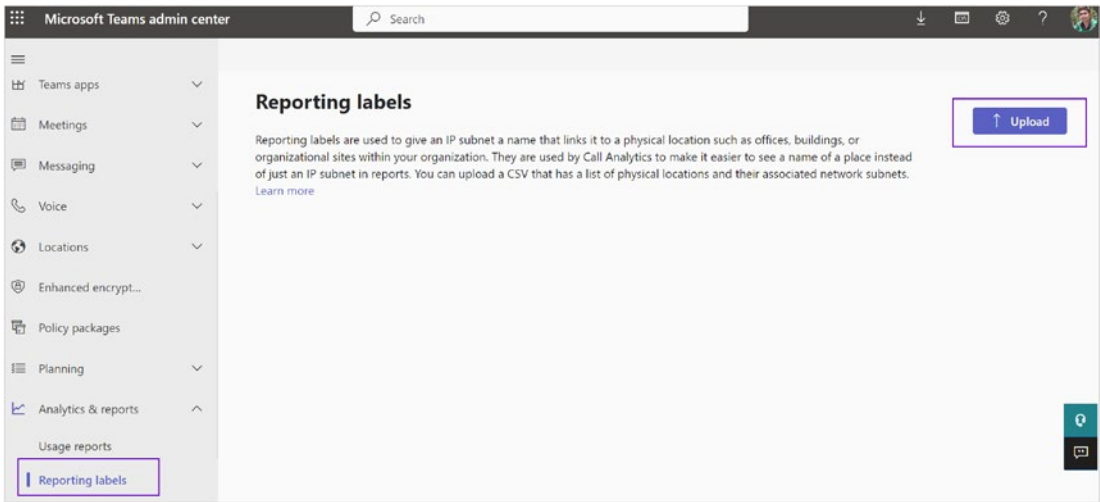


Figure 2-123. Upload Locations Data option

Once you click Upload Locations Data, you will see a new window where you can upload the location information with IP subnets using a labels file in .csv or .tsv format. I recommend downloading the existing template and then updating it and uploading it so that you will see any error while uploading the file.

Admin Center: Call Quality Dashboard

The Call Quality Dashboard (CQD) provides an overall view for analyzing Teams call quality. It supports Teams admins and network engineers in troubleshooting call quality problems with specific calls and helps them optimize a network. The users' individual call details are not visible in CQD, but the overall quality of calls made using Teams is captured. Another important use of CQD is to assess details about the audio and video call quality users are getting using Teams. It provides reports about call quality metrics that give you insights into overall call quality, server-client and client-client streams, and voice quality service-level agreements.

Using the Call Quality Dashboard

Microsoft Teams has extensive reporting and analytical capabilities that help admins to measure the overall call quality. When users report poor call quality, Teams and network admins can together check the CQD to see if an overall site-related issue could

be a contributing cause of the call quality problems. Microsoft has labeled many of the dimensions and measures as first or second. In the CQD, the main logic determines which endpoint involved in the stream or call is labeled as first.

- The first will always be considered the Teams Cloud service because the purely cloud-based Teams service means their server endpoints include Audio Video Multi-Control Unit (AV MCU), Mediation Server, transport relay, and so on. If a Teams service is involved in the stream or call, consider it as first.
- The second will always be a client endpoint unless the stream is between two server endpoints.
- If both endpoints are the same type, such as client–client, the order for which is first or second is based on the internal ordering of the user agent category. This ensures the ordering is consistent.

Note The first and second classification is separate from which endpoint is the caller or the person being called. The First Is Caller dimension can be used to help identify which endpoint was the caller or the person being called.

Accessing the Call Quality Dashboard

There are two CQD dashboards for Teams: one is a preview, and the other one is generally available. As an admin, you can access CQD through the Teams admin center, as well as directly by browsing to the CQD URL. Using the Teams admin center, log in to the Teams admin center and then navigate to and select Call Quality Dashboard. That will open a new browser tab for the Microsoft Call Quality Dashboard. To see the CQD, however, you need to sign in again. Once you sign in, you will see the CQD. Figure 2-124 shows the CQD displaying the overall call quality. You will see options to display the server–client call quality, client–client call quality, and voice quality SLA.

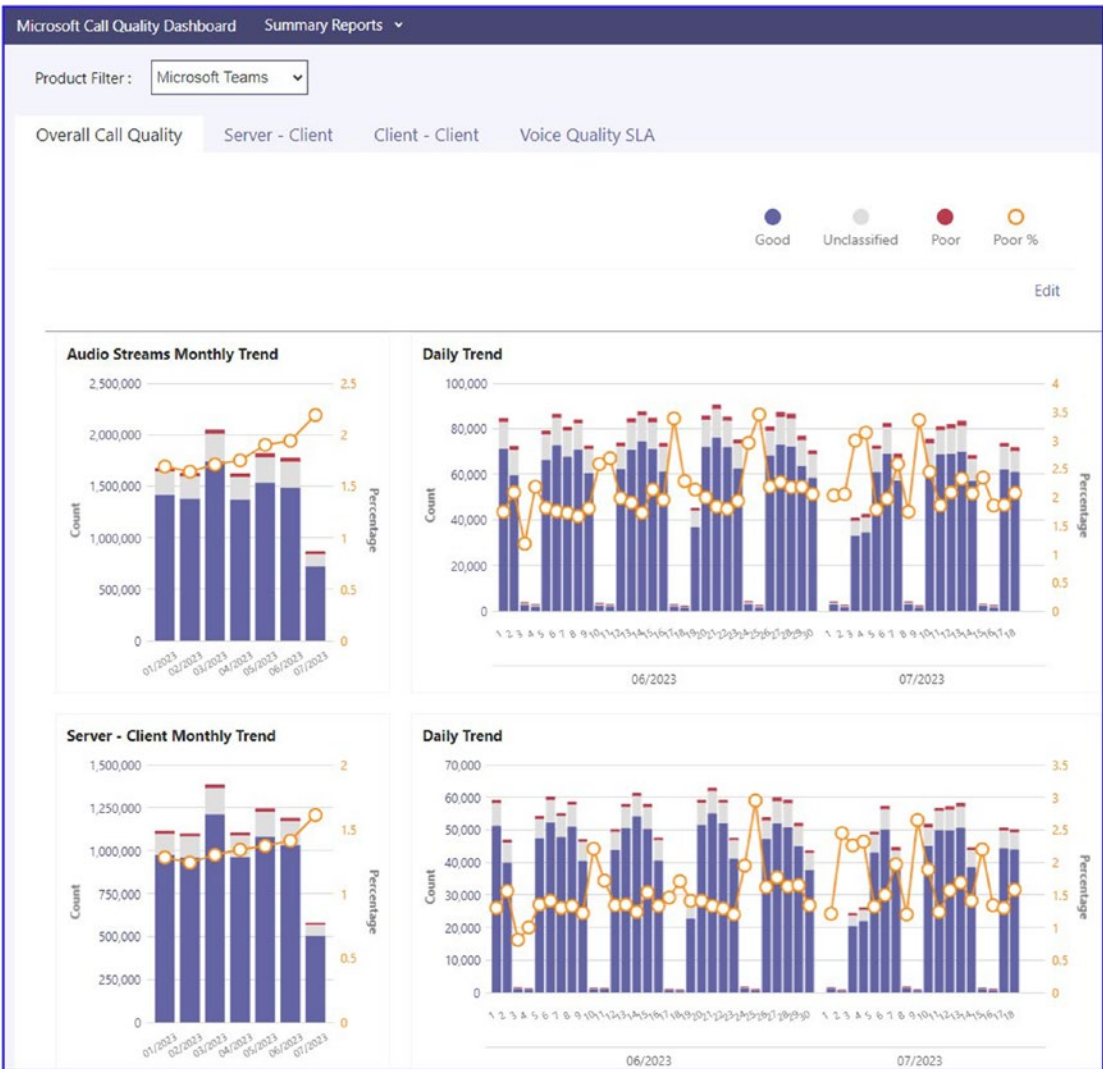


Figure 2-124. Call Quality Dashboard

You can see the CQD by directly browsing to <https://cq.d.teams.microsoft.com/spd/#/Dashboard>.

Displaying the List of Call Quality Reports

CQD provides multiple types of reports. Figure 2-125 shows the list of CQD reports on the Summary Reports tab. You can easily access each type of report by clicking its report name. To see the summary report, log in to the Teams admin center and then navigate to the CQD and then click it. It will open in a new browser tab.

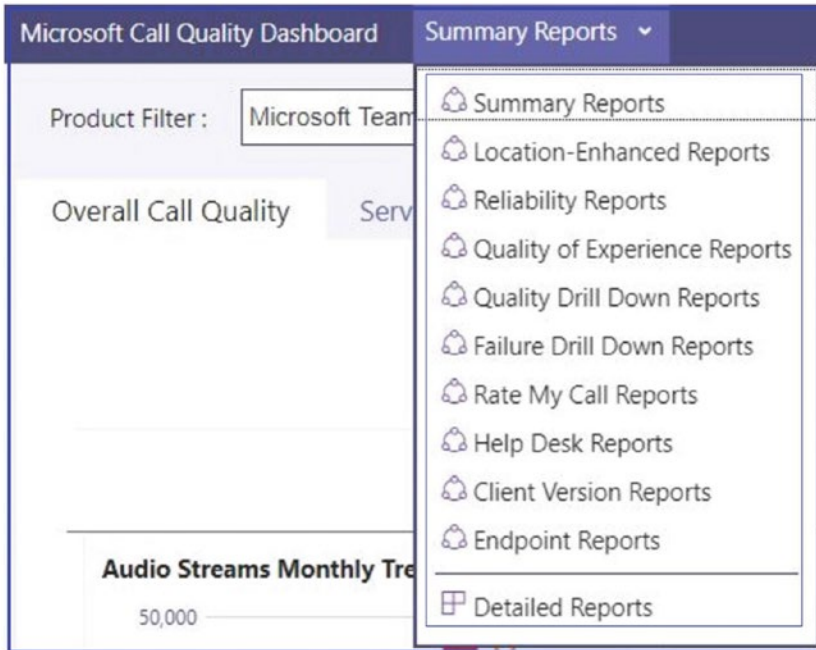


Figure 2-125. Summary Reports tab

Currently detailed reports are in preview. When you click Detailed Report, it opens and displays as a preview. To directly access the detailed report, simply visit <https://cqd.teams.microsoft.com/cqd/>. Figure 2-126 shows an example of a detailed report.

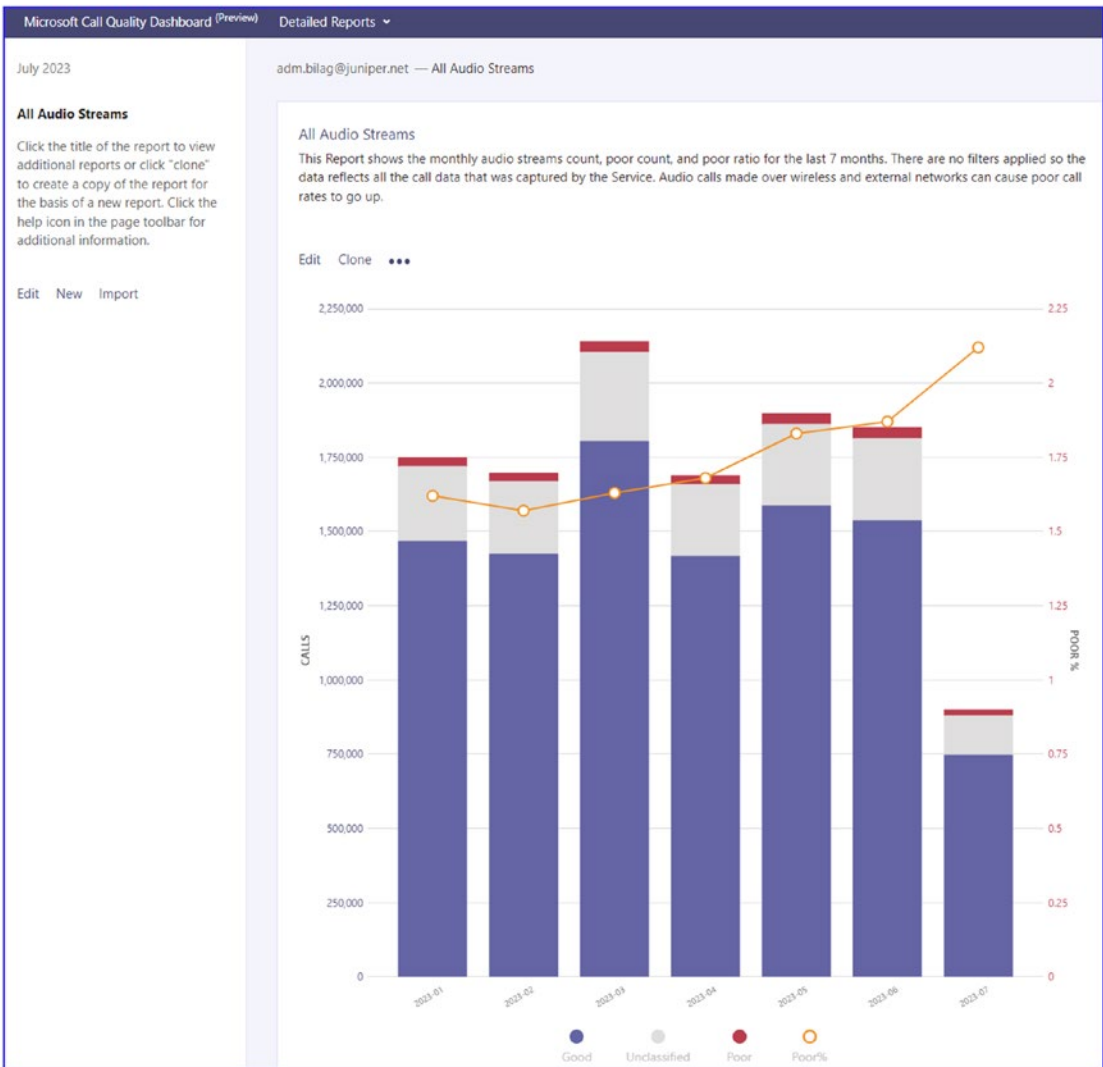


Figure 2-126. Detailed report for all audio streams

Click the title of the report to view additional reports or click Clone to create a copy of the report to use as the basis of a new report. For help, click the help icon on the page toolbar for additional information.

The All Audio Streams report in Figure 2-126 shows the monthly audio streams count ratio of and audio for the last seven months. There are no filters applied, so the data reflects all the call data captured by the Teams service. Audio calls made over wireless and external networks can cause poor call rates to go up.

Additional Tools for Teams Dependent Service Management

The following are additional tools.

Microsoft Azure Active Directory Center

In this section, you will learn about Azure AD usage within Teams. As a Teams admin, you must understand the role of directory services and identity management and that these came from Azure AD for Teams. Fundamentally, Azure AD is the cloud-based identity and access management service for Office 365. As such, it is an essential part of Microsoft Teams because Teams leverages identities stored in Azure AD for collaboration and communication. The license requirements for using Azure AD identities and for accessing Teams are included in a large number of different licensing packages, such as Small Business Plans like Office 365 Business, Enterprise Plans like Office 365 Enterprise E1/E3/E5, Education Plans like Office 365 Education, and Developer Plans like Office 365 Developer. This means almost every Office 365 plan includes Azure AD.

Microsoft Azure Active Directory (Azure AD) is a cloud-based identity and access management service, which helps your employees sign in and access resources in the following:

- External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization

Managing Microsoft Teams Identify

Managing identities in Microsoft Teams is closely linked with Azure Active Directory (Azure AD) as Teams relies on Azure AD for its identity service. This encompasses user identities, including guest users, bots, and system accounts. Here's how the identity management process typically works:

- **User provisioning:** When a user is created in Azure AD, they are automatically provisioned in Teams if they are licensed for it. The user details, such as name, email, etc., are pulled from Azure AD.

- **User authentication:** Teams uses Azure AD for authenticating users. This includes not only primary authentication when users sign in, but also MFA and conditional access policies to provide additional layers of security.
- **Role-based access control (RBAC):** Azure AD also provides role-based access control to Teams, allowing you to assign roles to users with specific permissions. For example, Teams has roles such as Owners, Members, and Guests, each with different levels of permissions.
- **Guest access:** Teams supports guest access, which lets you add individuals to your teams who are outside your organization. Guest users are added to Azure AD and sign into Teams using their own credentials, and their identity is managed in Azure AD.
- **Security and compliance:** Teams, in conjunction with Azure AD, provides various security and compliance features such as data loss prevention (DLP), eDiscovery, legal hold, and more.

Managing identity is the biggest challenge for any cloud application deployment, and Teams is no exception. When designing and deploying cloud applications, one of the biggest challenges is how to manage the login credentials in the application for authenticating to cloud services while keeping users' credentials secure. Azure AD resolves this problem with a feature called *managed identities*, which provides access to Azure and Office 365 resources for custom applications and services. As previously mentioned, Microsoft Teams leverages Azure AD for identity management. The feature provides Azure services with an automatically managed identity in Azure AD. As an admin, you can use this identity to authenticate to any service that supports Azure AD authentication, such as Microsoft Teams, Exchange Online, SharePoint, OneDrive, and Yammer without any credentials in the application code.

Azure AD has multiple features that provide granular control to Teams admins, such as Azure AD access review, which allows organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. Conditional access is the set of rules for access control based on various specifications such as client, service, registration procedure, location, compliance status, and so on. Conditional access is used to choose whether the user's has access to the organization data.

In addition, Teams provides additional settings for managing user experiences and policies at the team and channel levels, which include things such as team creation policies, app setup policies, meeting policies, etc.

Remember that the ability to manage identities in Microsoft Teams, such as creating and assigning roles, implementing policies, etc., requires administrative privileges. Administrators can access these controls via the Microsoft Teams admin center or through PowerShell commands.

Accessing Azure AD

Accessing the Azure AD portal can be done with these simple steps:

1. **Open a web browser:** Open your preferred web browser.
2. **Navigate to the Azure portal:** Type in the following URL into your web browser: <https://portal.azure.com/>. Or log in to the Microsoft 365 admin center by browsing to <http://portal.office.com/> and then clicking Admin or directly visiting the admin portal URL at <https://admin.microsoft.com/Adminportal/Home>. Then click Azure AD.
3. **Sign into your account:** Click the Sign In button. You'll be directed to the Microsoft sign-in page.
4. **Enter your credentials:** Type in your Microsoft credentials, which is typically your email or phone number, and click Next. Then enter your password.

Note If you have MFA enabled, you will need to verify your identity using the method you've set up (e.g., a phone call, text message, or an app notification).

5. **Access the Azure Active Directory:** Once logged in, you'll see the main Azure dashboard. On the left side, there's a navigation pane. Look for Azure Active Directory and click it. If it's not visible, click All Services, and search for *Azure Active Directory*. You can also pin Azure Active Directory to the sidebar for easy access in the future.

6. **Explore Azure Active Directory:** Now you should be in the Azure AD interface, where you can manage users and groups, handle identity protection and security, define user settings, etc.

Once the Microsoft 365 admin center page opens, click Show All to show all the admin tools and then select Azure Active Directory. Once the Azure AD admin center page opens, click Azure Active Directory to show the Azure AD capabilities.

Using Azure AD, as an admin you can manage users, groups, organizational relationships, roles and administrators, devices, and so on. Figure 2-127 shows the Azure AD admin center for the Bloguc organization.

Complete details about Azure AD are outside the scope of this book. I provide the summary of Azure AD here, though, because Microsoft Teams leverages Azure AD for identity management.

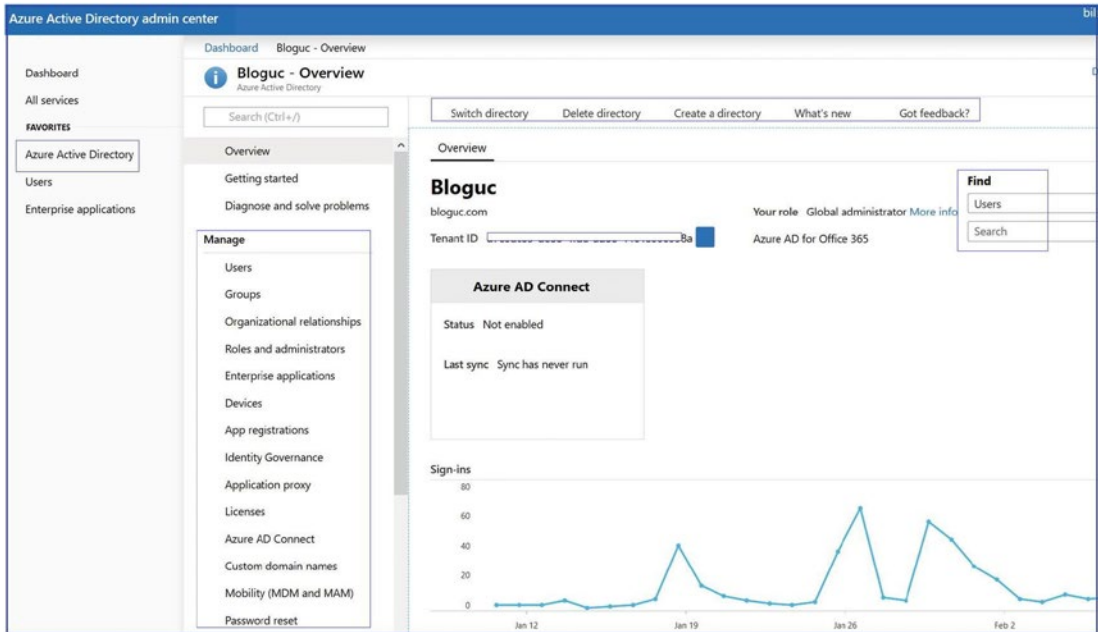


Figure 2-127. Azure Active Directory admin center

Microsoft 365 Admin Center

The Microsoft 365 admin center is the main portal where administrators can manage all their Microsoft services. It allows them to set up users, manage licenses, configure security settings, manage resources, and access support, among other administrative tasks.

You can create users or Office 365 groups and manage them through the Microsoft 365 admin center. Figure 2-128 shows the Microsoft 365 admin center. Again, complete details of the Microsoft 365 admin center are outside the scope of this book. I provide brief information about the Microsoft 365 admin center here because Teams and add-on Phone System licenses are assigned and managed, and Teams usage reports are available through the Microsoft 365 admin center.

Accessing Microsoft 365 Admin Center

Accessing the Microsoft 365 admin center can be done as follows:

1. **Open a web browser:** Open your preferred web browser.
2. **Navigate to the Microsoft 365 admin center:** Enter the following URL into your web browser: <https://admin.microsoft.com/>.
3. **Sign into your account:** Click the Sign In button. You'll be directed to the Microsoft sign-in page.
4. **Enter your credentials:** Enter your email, phone, or Skype credentials. These credentials must be associated with an account that has administrative privileges in Microsoft 365. Then, click Next. Enter your password and click Sign in.

Note If you have MFA enabled, you will need to verify your identity using the method you've set up (e.g., a phone call, text message, or an app notification).

5. **Access the Microsoft 365 admin center:** Once you sign in, you'll be directed to the main dashboard of the Microsoft 365 admin center.

- 6. **Explore the Microsoft 365 admin center:** From here, you can manage users and groups, billing, licenses, admin centers for all Microsoft services, and a whole lot more. You can use the Microsoft 365 admin center to assign Teams, Exchange, SharePoint licenses, and user management.

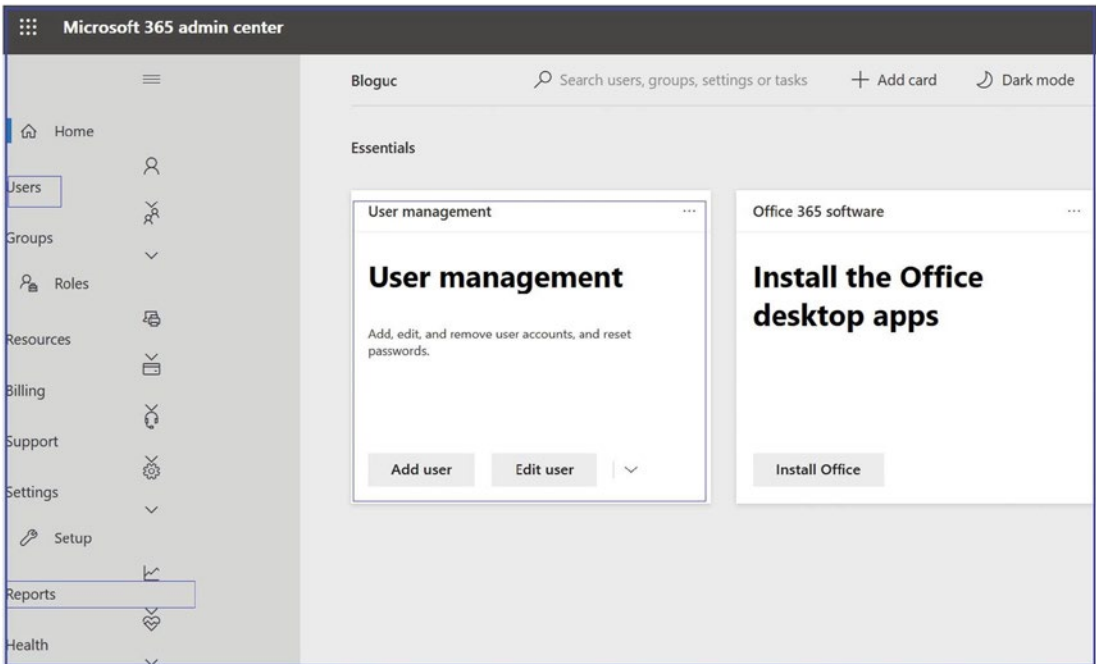


Figure 2-128. Microsoft 365 admin center

Remember, not all users in a Microsoft 365 organization have access to the admin center. You need to have administrator privileges for your organization to access the admin center. If you don't have admin privileges, you'll see a message that you don't have permission to access the page. In such cases, you should contact your organization's IT administrator.

Accessing Teams Reports in the Microsoft 365 Admin Center in the Reports Dashboard

The Microsoft 365 admin center is a portal where administrators can manage all Microsoft services, including users, groups, billing, licenses, and a wide range of settings and configurations.

Under the Reports section in the Microsoft 365 admin center, administrators can gain insights into how users in the organization are utilizing Microsoft 365 services. There is a Usage section under Reports that allows you to view different usage data.

Here are some of the types of usage reports you might see:

- **Microsoft 365 active users:** This report shows the number of active users that perform an activity using any Microsoft 365 or Office 365 product.
- **Microsoft 365 services usage:** Here you can see the usage details of individual Microsoft services such as Exchange (email), OneDrive, SharePoint, Teams, and Yammer.
- **Email activity:** This report shows statistics on email usage, including the volume of sent/received mail, and the number of active users.
- **OneDrive activity:** This report gives details about how users in your organization are using OneDrive, such as file count, storage used, and sharing activity.
- **SharePoint activity:** This report provides insights into how users are utilizing SharePoint, including file usage, active sites, and storage metrics.
- **Teams activity:** You can get insights on how your organization is using Teams, such as the number of active users, meeting participation, and calling and chat usage.
- **Yammer activity:** This report will tell you about Yammer usage, including the number of posts, reads, and likes.

The reports provide information about how your Teams deployment is being used and how users are taking advantage of Teams for their collaboration and communication needs. While you are managing a Microsoft Teams environment as an admin within your

organization, you will need to generate the usage report from the Microsoft 365 admin center to see how the users in your organization are using Microsoft Teams. These usage and activity reports provide you with comprehensive information to choose where to prioritize training and communication efforts. Using the Microsoft 365 admin center, you can view two activity reports: the Microsoft Teams device usage report and the Microsoft Teams user activity report.

1. To view the Teams user activity and device usage reports, log in to the Microsoft 365 admin center, select Reports, and then select Usage.
2. Once the Usage page opens, click “Select a report,” and then click Microsoft Teams. Select Device Usage or User Activity to choose the report you want to view.
3. You can then analyze the report, as shown in Figure 2-129.

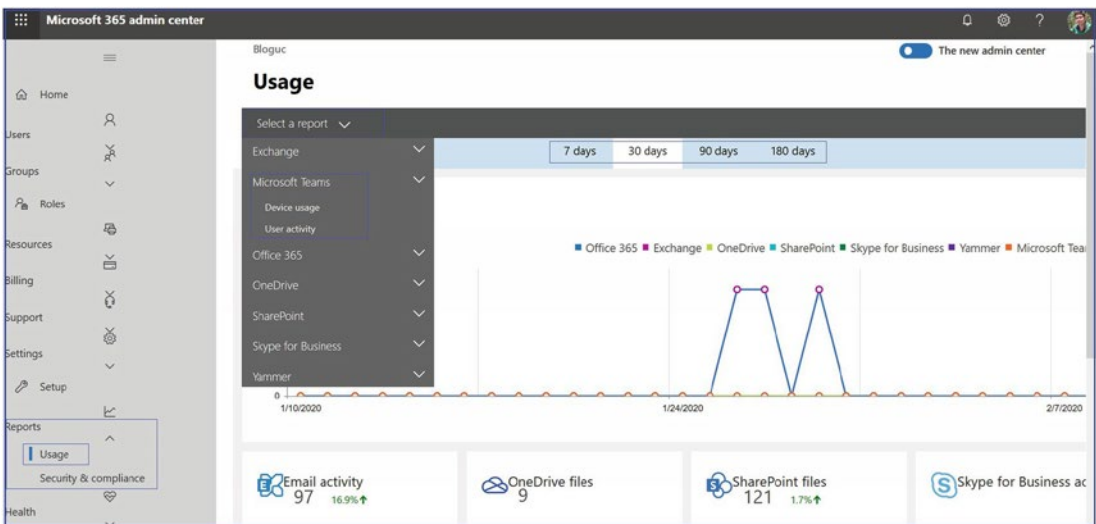


Figure 2-129. Teams usage reports

Remember that to view the activity reports, you need one of the following admin role permissions:

- Global administrator
- Exchange administrator

- SharePoint administrator
- Reports reader (the Reports reader role can be assigned to a non-IT user who you would like to have access to these reports by assigning this role)

Remember, these reports can be filtered and adjusted by date range and other factors, and many of them can be downloaded for offline use or further analysis. Please note that your ability to view certain reports might depend on your role and permissions within the organization.

Microsoft 365 Security and Compliance Centers

The Microsoft 365 Security Center and the Microsoft 365 Compliance Center are specialized dashboards that offer administrators unified experiences to manage and enhance the security and compliance of their organizations.

Microsoft 365 Security Center

The Microsoft 365 Security Center is designed to help you manage and enhance the security posture of your organization. It's a central place where you can monitor and respond to security incidents and set up security policies across Microsoft 365.

Here's what you can do in the Security Center:

- **Threat management:** Monitor and manage real-time threat incidents across your Microsoft 365 organization.
- **Alerts dashboard:** View and manage security alerts.
- **Secure score:** Evaluate your organization's security posture by giving you visibility into your existing security settings and providing recommendations to enhance security.
- **Security policies:** Configure various security policies like Safe Links, Safe Attachments, Anti-Spam, and more.
- **Investigate risks:** Use advanced hunting to query across your data to identify potential risks.
- **Manage Devices:** If integrated with Microsoft Endpoint Manager, you can manage the security of devices used within your organization.

Microsoft 365 Compliance Center

The Microsoft 365 Compliance Center is a specialized dashboard for managing the compliance needs of your organization. It gives you a centralized place to access solutions that help you comply with standards, regulations, and laws.

Here's what you can do in the Compliance Center:

- **Compliance Manager:** Understand, manage, and improve your organization's compliance posture with regard to various regulations and standards such as GDPR, ISO 27001, etc.
- **Data subject requests:** Respond to data subject requests for GDPR and other regulations.
- **Data classification:** Classify your data based on sensitivity labels and retain it using retention labels.
- **Data loss prevention (DLP):** Create, manage, and monitor DLP policies to protect sensitive information.
- **eDiscovery:** Search for content across Microsoft 365 for legal and compliance purposes.
- **Audit logs:** Access and search the audit log for user and administrator activities across Microsoft 365.
- **Insider risk management:** Identify risky activities within your organization and take appropriate action.

The advanced security capabilities of Microsoft Teams help you create policies to secure your information and protect company data. Microsoft provides and displays the latest features that enable secure collaboration while helping customers meet their obligations under national, regional, and industry-specific regulations. Microsoft Teams is one of the fastest growing apps in Microsoft history.

As a Teams admin and compliance and information security admin in your organization, you must be aware of what Teams provides to securely maintain the data that Microsoft Teams generates. When the data are generated, admins' concerns are who is accessing the Teams data and how it can be secured and accessed by the right set of users who need the data.

Microsoft is heavily investing in securing the Teams data, and Teams is a first-party application that applies all the security, compliance, and identity investments that Microsoft has already made in information protection and compliance.

Most people believe that ineffective communication is the cause for workplace failures. There is a long list of applications that provide communication and collaboration, but they are lacking the facet of helping people come together, be more productive, and allow them to do everything that they want to do. That's where Microsoft Teams comes in.

Microsoft Teams is a hub for teamwork, as everything that a team requires is in one place such as chats with threaded conversation, meetings with voice and video conferencing and application sharing, calls with voice and video and PSTN phone calls, files for collaboration, and applications and workflows that allow users to create and integrate your application in one frame. These features are all crucial for teamwork, and Microsoft Teams provides everything that users need to do their day-to-day work in more productive ways.

To understand the Teams security and compliance capabilities, it is important to separate queues such as identity and access management, information protection, the ability to discover content and respond to it, the application of data governance policies for the type of content that exists, the duration, and finally the ability to manage risks.

Remember, access to these centers requires the necessary permissions and privileges, so not all users will be able to access or perform all tasks in these centers.

Understanding Identity and Access Management for Teams

Identity and access management (IAM) in the context of Microsoft Teams is a set of business processes and supporting technologies that help ensure the right people have access to the right parts of Teams. It is closely tied to Azure AD, the identity provider for Microsoft 365 that includes Teams.

Here are some key aspects of IAM for Teams:

- **Identity:** An identity is the digital representation of a user in an organization. In Teams, a user's identity includes their username, password, roles, groups, and other attributes. Identities in Teams are managed via Azure AD. When a user is created in Azure AD and assigned a Teams license, they become a Teams user.

- **Authentication:** Authentication is the process of validating a user's identity. When a user signs into Teams, they're authenticated by Azure AD. Azure AD supports various types of authentication methods, including password-based, MFA, and more.
- **Authorization:** Authorization is the process of determining what a user can do in Teams after they've been authenticated. For example, a user might be authorized to join a team, create a channel, or initiate a meeting. In Teams, authorization is managed through various settings and policies in the Teams admin center.
- **Access management:** Access management involves defining and managing the access that users have in Teams. This includes things such as setting up guest access (allowing people outside the organization to join Teams), setting up sharing policies (controlling how users in Teams can share files and content), and setting up meeting policies (controlling who can create meetings, who can join, etc.).
- **RBAC:** In Teams, roles are used to control what users can do. There are several built-in roles in Teams, including Owner, Member, and Guest, each with different levels of permissions. Owners have the most permissions, including the ability to add and remove members, update team settings, and more. Members have fewer permissions but can still interact fully within the team, and Guests have the fewest permissions.
- **Security:** Teams leverages the security features of Azure AD to protect user identities and data. This includes features such as MFA, conditional access policies, identity protection, and more.

Understanding IAM for Teams can help ensure that the right people have the right access in Teams, enhancing both productivity and security.

Identities are key for any application or system. If bad actors compromise an identity, your data and content are at risk. Because Teams leverages Azure AD for identity, the investments and improvements that have occurred in Azure are directly applied to Microsoft Teams.

Does Teams have robust authentication? Teams has solid authentication because Teams uses smart protection policies and risk assessment to block threats. As an admin, you need to ensure that your organization's users have strong passwords and have MFA enabled. Once you have enabled MFA for SharePoint Online and Exchange Online, you automatically endorsed it for Teams because Teams used SharePoint and Exchange extensively. When users try to log in to Teams, they will challenge for the two-factor workflow or whether you have a PIN enabled; both have the same workflow.

Another aspect is what to authorize a user to access. This is specifically based on a policy that is defined in conditional access in Azure AD, and Microsoft Teams is part of this feature as well. Conditional access flow is based on the signal that comes from the devices, applications, and users. Microsoft determines a risk score, and as an admin you configure the policies that determine who can access the Teams application.

Remember, the conditional access policies prevent access for authenticated users from unmanaged devices. Understanding IAM for Teams can help ensure that the right people have the right access in Teams, enhancing both productivity and security.

Accessing the Office 365 Security & Compliance Center

As a Teams admin and compliance and information security admin, you must be aware of what the Microsoft 365 Security & Compliance Center provides for Teams to securely maintain the data that Microsoft Teams generates. You can also use classification labels, data loss prevention (DLP), information governance, and so on. To access the Office 365 Security & Compliance Center, log in to Office 365 admin center and then click Security & Compliance to open the Office 365 Security & Compliance Center, as shown in Figure 2-130. You can also directly access the Security & Compliance Center by visiting <https://compliance.microsoft.com/>.

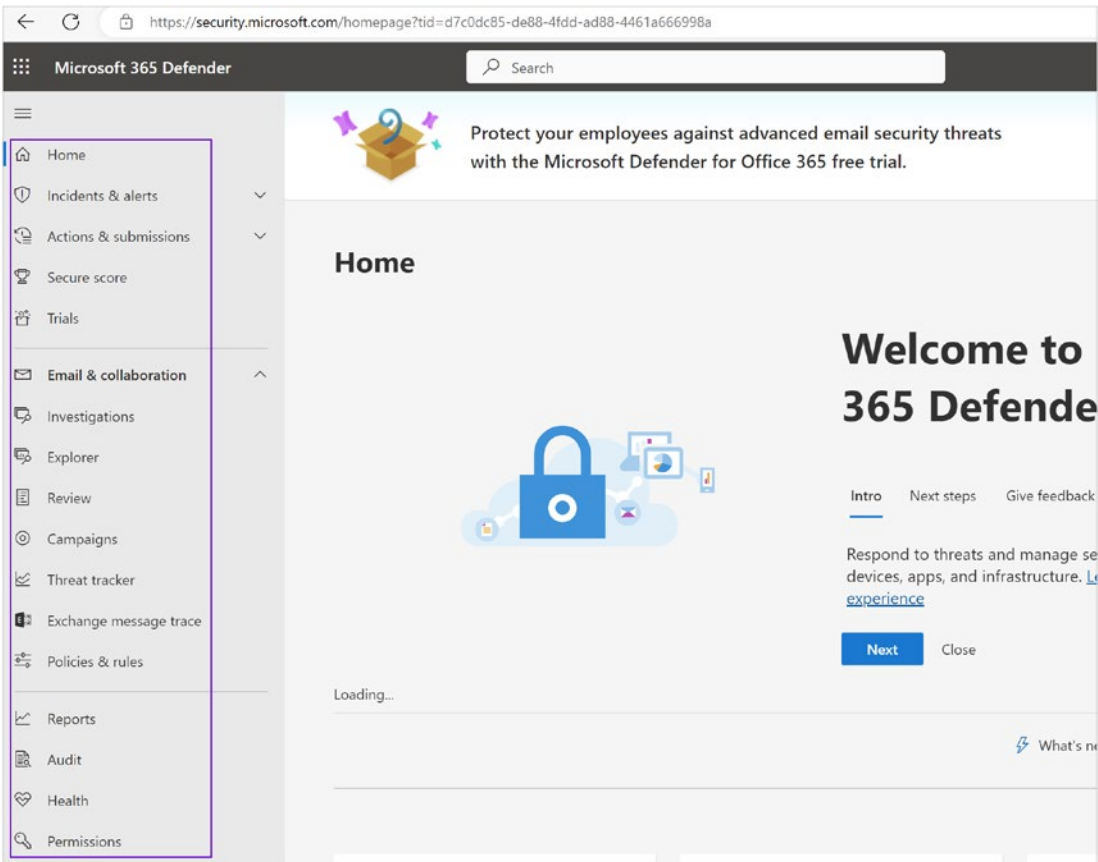


Figure 2-130. Microsoft 365 Security Center

Figure 2-131 shows Microsoft 365 Compliance Center.

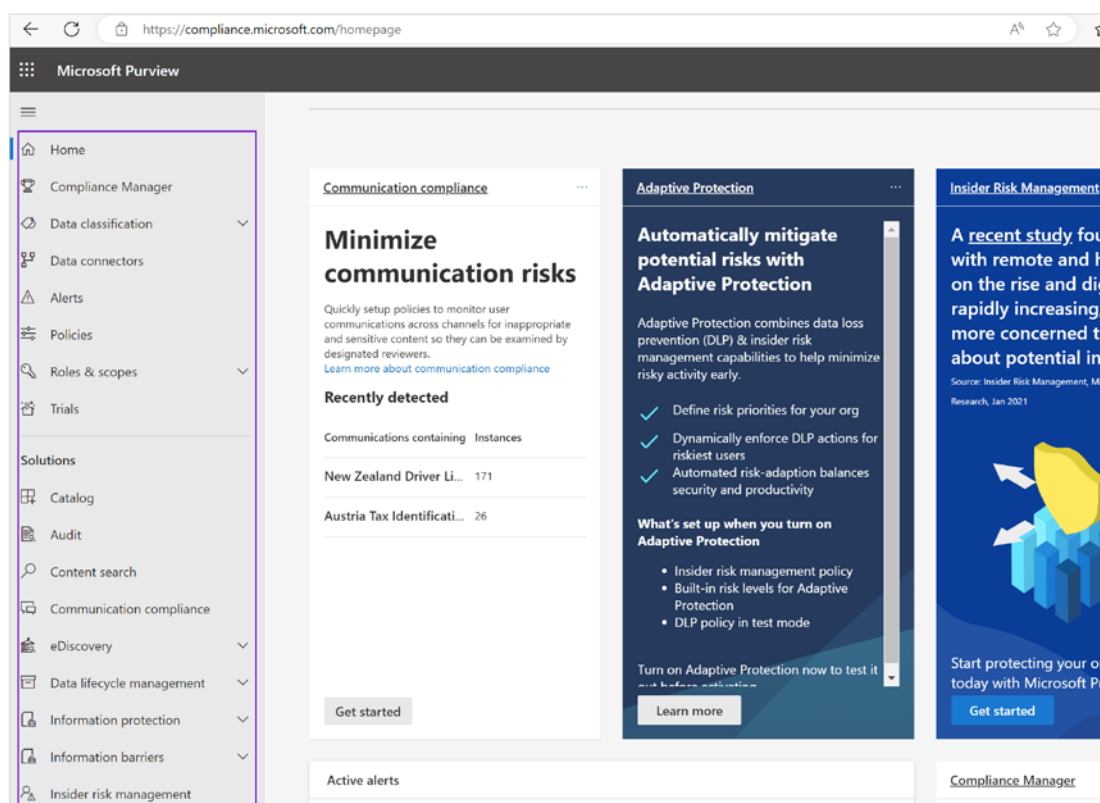


Figure 2-131. Microsoft 365 Compliance Center

Topics such as managing sensitivity labels and data loss prevention policies, managing eDiscovery cases and supervision policies, configuring alert policies for events in Microsoft Teams, and creating retention policies and information barriers are covered in Chapter 5.

Teams Management Through PowerShell

PowerShell is a powerful command-line shell and scripting language that provides Teams administrators with control and automation of Teams management tasks. Teams administrators can use the Teams PowerShell module to manage various aspects of Teams, including managing Teams settings, policies, users, and more.

Before you use PowerShell for Teams, you need to install the Teams PowerShell module. To do this, open PowerShell as an administrator and run the following command:

Note Update to Windows PowerShell 5.1. If you're on Windows 10 version 1607 or higher, you already have PowerShell 5.1 installed and can install .NET Framework 4.7.2 or later as prerequisites.

```
Install-Module -Name PowerShellGet -Force -AllowClobber
```

Then, you can install the Teams PowerShell module with the following command:

```
Install-Module -Name Teams -Force -AllowClobber
```

After installing the Teams PowerShell module, you need to connect to the Teams service in PowerShell. Here is how you do it:

```
# Import Teams module
Import-Module Teams

# Get credential
$credential = Get-Credential

# Connect to Microsoft Teams
Connect-MicrosoftTeams -Credential $credential
```

Once connected, you can use various cmdlets to manage Teams. Here are some commonly used PowerShell cmdlets for Teams:

Get-Team: Retrieves all the teams a user is part of

```
Get-Team -User user@bloguc.com
```

New-Team: Creates a new team

```
New-Team -DisplayName "New Team" -Description
"Description of the new team"
```

Add-TeamUser: Adds a user to a team

```
Add-TeamUser -GroupId teamGroupId -User
user@bloguc.com -Role Member
```

Remove-TeamUser: Removes a user from a team

```
Remove-TeamUser -GroupId teamGroupId -Use user@bloguc.com
```

Set-Team: Modifies the settings of a team

```
Set-Team -GroupId teamGroupId -DisplayName "Updated Team Name"
```

Get-TeamChannel: Retrieves all the channels for a team

```
Get-TeamChannel -GroupId teamGroupId
```

New-TeamChannel: Creates a new channel in a team

```
New-TeamChannel -GroupId teamGroupId -DisplayName "New Channel  
Name" -Description "Description of the new channel"
```

Phone Number Assignment

Assigning a phone number to a user involves acquiring a phone number from Microsoft or porting your existing numbers and then assigning it to a user. You can use the `Set-CsPhoneNumberAssignment` cmdlet to assign a phone number to a user with Direct Routing:

```
Set-CsPhoneNumberAssignment -Identity user@bloguc.com -PhoneNumber  
+12091234567 -PhoneNumberType DirectRouting
```

Voice Policy Assignment

Voice policies define what calling features are available to users. The `Grant-CsTeamsCallingPolicy` cmdlet can be used to assign a voice policy to a user:

```
Grant-CsTeamsCallingPolicy -Identity user@example.com -PolicyName  
"Calling Policy Name"
```

Dial Plan Assignment

Dial plans are used to normalize phone numbers for users. You can assign a dial plan to a user with the `Grant-CsDialPlan` cmdlet:

```
Grant-CsDialPlan -Identity user@example.com -PolicyName "Dial Plan Name"
```

Unassign

To unassign a policy or a phone number from a user, you can use the `Remove` cmdlet:

```
Remove-CsPhoneNumberAssignment -Identity user@example.com -PhoneNumber  
+12065551234  
Remove-CsTeamsCallingPolicy -Identity user@example.com  
Remove-CsDialPlan -Identity bilag@bloguc.com
```

Teams Meeting Management

Here are some cmdlets for managing Teams meetings.

To get information about Teams meeting policies, use this:

```
Get-CsTeamsMeetingPolicy -Identity "Meeting Policy Name"
```

To assign a Teams meeting policy to a user, use this:

```
Grant-CsTeamsMeetingPolicy -Identity user@example.com -PolicyName "Meeting Policy Name"
```

Teams Live Event Management

Here are some cmdlets for managing Teams Live events.

To get information about Teams Live event policies, use this:

```
Get-CsTeamsLiveEventPolicy -Identity "Live Event Policy Name"
```

To assign a Teams Live event policy to a user, use this:

```
Grant-CsTeamsLiveEventPolicy -Identity user@example.com -PolicyName "Live Event Policy Name"
```

Teams Room System Management

Here are some cmdlets for managing Teams Rooms.

To get information about Teams room devices, use this:

```
Get-CsTeamsRoom -Identity "Room System Name"
```

To set properties of a Teams room device, use this:

```
Set-CsTeamsRoom -Identity "Room System Name" -DisplayName "New Room Name"
```

Remember, you should replace bilag@bloguc.com, +12091234567, Policy Name, Dial Plan Name, and Room System Name with actual values. Be sure to also check Microsoft's documentation to understand the requirements and impacts of these commands.

PowerShell provides Teams administrators with granular control over Teams management tasks and can be a very efficient way of managing Teams, especially for large organizations or for repetitive tasks. PowerShell can also be used to automate various Teams management tasks by writing scripts that run these cmdlets in sequence or on a schedule.

Summary

This chapter provided a comprehensive overview of the diverse tools available for managing and controlling Microsoft Teams. It underscores the significance of the Teams admin center as the primary portal for administering Teams and outlines its various functionalities, from managing teams, channels, and apps to adjusting settings and policies.

In addition to the Teams admin center, the chapter discussed the role of the Microsoft 365 admin center in managing users and groups, licensing, and organization-wide settings. It highlighted the seamless integration of these platforms, enabling efficient user and resource management across Microsoft 365 services.

Next, the chapter explored Azure AD and its integral role in Teams management. Azure AD's central position in handling user identities, authentication, and access control was thoroughly discussed. The chapter elucidates how Azure AD policies can impact Teams, including user sign-ins, guest access, and group memberships.

Following Azure AD, the chapter delved into the use of PowerShell for Teams administration. It illustrated how administrators can leverage PowerShell to automate repetitive tasks, carry out bulk operations, and implement advanced management tasks that are not possible through the admin centers. A variety of common PowerShell commands for Teams were also presented as examples.

Finally, the chapter wrapped up with a detailed examination of the Microsoft Security & Compliance Centers. It explained how these tools are used to enforce security and compliance across Teams and the entire Microsoft 365 suite. The features of these centers, such as threat management, data loss prevention, data governance, and audit log investigations, were thoroughly explained.

In conclusion, this chapter gave administrators a comprehensive toolkit for managing and controlling Microsoft Teams effectively. From day-to-day tasks such as user and team management to advanced security and compliance enforcement, administrators now understand how to utilize these tools to ensure a secure and productive Teams environment.