



Understanding Microsoft Teams Administration

Configure, Customize, and Manage
the Teams Experience

—
Balu N Ilag

Apress®

Understanding Microsoft Teams Administration

Configure, Customize, and Manage
the Teams Experience

Balu N Ilag

Apress®

Understanding Microsoft Teams Administration: Configure, Customize, and Manage the Teams Experience

Balu N Ilag
Tracy, CA, USA

ISBN-13 (pbk): 978-1-4842-5874-3
<https://doi.org/10.1007/978-1-4842-5875-0>

ISBN-13 (electronic): 978-1-4842-5875-0

Copyright © 2020 by Balu N Ilag

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Smriti Srivastava
Development Editor: Matthew Moodie
Coordinating Editor: Shrikant Vishwakarma

Cover designed by eStudioCalamar

Cover image designed by Pexels

Distributed to the book trade worldwide by Springer Science + Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit <http://www.apress.com/rights-permissions>.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-5874-3. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

*This book is dedicated to
my mother, Chandrabhaga. Today, what I am is because of you,
and I know you are always with me wherever I go.
I really miss you, Bai.*

*And to my wife Vaishali, who has always accepted me and supported
me in good and bad times. You are and always will be my perfect wife
and mommy to our beautiful princesses, Shravya and Chanda.
So, all I say is thank you, Vaishu.*

Table of Contents

About the Author	xiii
About the Technical Reviewer	xv
Acknowledgments	xvii
Introduction	xix
Chapter 1: Microsoft Teams Overview	1
What Is Microsoft Teams?	2
Microsoft Teams Architecture	2
Teams Architecture Overview	3
What Is the Intelligent Communications Cloud?	4
Microsoft Office 365 Services Used by Teams	5
Microsoft Teams Capabilities and Their Data Storage Locations	7
Microsoft Teams Logical Architecture	8
Microsoft Teams Depends on Other Services	10
Microsoft Teams Teams and Channels	11
Teams	11
Channels	13
How Does Microsoft Teams Manage Identities?	15
Tabs, Files, and Connectors in Teams	16
Tabs	16
Files	17
Microsoft Stream and Live event	17
Microsoft Stream Architecture	17
Where Is My Stream Data Residing?	20
Microsoft Teams Live Event	20

TABLE OF CONTENTS

- Teams Voice and Video Call and Meetings 28
 - Teams Voice and Video Calls 28
 - Microsoft Teams Meetings 29
 - Who Can Attend the Teams Meeting? 31
- Teams Phone System Overview 32
 - What Does the Phone System Require? 32
- Microsoft Teams Licensing Requirement Overview 33
- Teams Integration with a Third-Party Application 35
- Summary..... 36
- Chapter 2: Managing and Controlling Microsoft Teams 37**
 - Microsoft Teams Authentication..... 38
 - How Microsoft Teams User Authentication Works 38
 - Microsoft Teams Sign-in Process 39
 - Manage and Configure Multifactor Authentication and Conditional Access for Teams..... 41
 - What Is Conditional Access in Authentication?..... 41
 - How Conditional Access Flow Works..... 41
 - Managing Teams, Channels, and Their Types..... 42
 - Creating a Channel in a Team..... 47
 - Deploying and Managing Teams Clients 58
 - Installing Teams Client on Desktop and Mobile? 58
 - Getting the Teams Client Download for All Devices 59
 - Teams Desktop Client Software and Hardware Requirements..... 60
 - Teams Desktop Client for Windows 60
 - Managing Teams Desktop Client 63
 - Configuring and Managing Live Events and Microsoft Stream 67
 - Overview of Live Events 68
 - Configuring and Managing Live Events Settings 69
 - Managing Microsoft Stream 74
 - Organizing and Managing Groups and Channels in Stream 75

Administrative Tools	76
Managing Teams Using Microsoft Teams Admin Center	76
Teams Administration Through Teams Admin Center	78
Admin Center: Devices Tab	82
Admin Center: Locations Tab	91
Admin Center: Users Tab	98
Admin Center: Meetings Tab	99
Admin Center: Messaging Policies Tab	109
Admin Center: Teams Apps Tab	114
Admin Center: Voice Tab	126
Microsoft Azure Active Directory Center	218
Managing Microsoft Teams Identify	219
Accessing Azure AD	219
Microsoft 365 Admin Center	220
Accessing Microsoft 365 Admin Center	221
Accessing Teams Reports in Microsoft 365 Admin Center in the Reports Dashboard	221
Office 365 Security & Compliance Center	223
Understanding Identity and Access Management for Teams	224
Accessing the Office 365 Security & Compliance Center	224
Teams Management Through PowerShell	225
Summary	229
Chapter 3: Organization Readiness for Microsoft Teams	231
Network Assessment and Bandwidth Planning for Teams	232
Carrying Out a Network Assessment Before Teams Deployment	233
Network Bandwidth Requirements for Microsoft Teams Calling Scenarios	236
Network Planner	237
Network Testing Companion Tool	241
Deploying and Managing Quality of Service	246
Deploying Quality of Service for Microsoft Teams	247
Applying DSCP Marking at Network Layer	248

TABLE OF CONTENTS

- DSCP Marking at Endpoint Level Using Policy-Based QoS 248
- Verifying QoS Policies Are Applied..... 256
- Deploying VPN Split Tunnel for Microsoft Teams Media Traffic 257
 - Understanding Split-Tunnel VPN for Teams Media Traffic..... 257
 - Split-Tunnel VPN Architecture..... 258
 - Implementing Split-Tunnel VPN 259
 - Verifying VPN Split Tunneling..... 261
- Summary..... 262
- Chapter 4: Teams Audio Conferencing and Phone System Management 263**
 - Planning and Managing Teams Conferences 264
 - Microsoft Teams Conferences 264
 - Organizing Teams Meetings Efficiently..... 265
 - Teams Meeting Attendee Types 270
 - Meeting Attendees' Experience 271
 - Recording with Microsoft Stream..... 272
 - Microsoft Teams Meeting Networking Considerations 273
 - Where Teams Meetings Are Hosted 273
 - Networking Considerations for Teams Meeting Deployment..... 273
 - Allowing Teams Inbound and Outbound Traffic Through Firewall Configuration 274
 - Managing a Teams Meeting..... 275
 - Creating and Managing Meeting Policy 276
 - Checking Teams Meeting Quality 280
 - Microsoft Teams Audio Conferencing..... 281
 - Teams Audio Conferencing Licensing Requirements..... 282
 - Teams Audio Conferencing Requirements..... 283
 - Adding Additional Dedicated Conference Bridge Numbers 284
 - Setting a Default Conference Bridge Number 284
 - Configuring and Managing Teams Conference Bridge Settings 285
 - Setting Up and Managing Communications Credits for Audio Conferencing..... 286
 - Assigning Communications Credits to a User..... 288
 - Configuring and Managing Meeting Policies 292

Teams Phone System Planning.....	293
Configuring and Managing Teams Direct Routing	294
Configuring and Customizing Online PSTN Gateway for Microsoft Teams Direct Routing.....	295
Configuring and Managing Teams Calling Plans	301
Configuring and Managing Call Queue	305
Managing and Configuring Auto Attendant in Teams.....	312
Configuring and Managing Emergency Calling.....	322
Managing Phone Numbers	334
Creating and Managing Voice Routing Policy.....	336
Summary.....	339
Chapter 5: Microsoft Teams Governance and Life Cycle Management.....	341
User Provisioning for Microsoft Teams	342
Enabling a User Teams License	342
Assigning Meeting Policy to a User Account Using Teams Admin Center.....	343
Third-Party Application and Policy Management.....	345
Teams Apps Permission Policies	346
Managing the Custom App Setup Policies.....	346
Assigning a Custom App Setup Policy to Users	347
Teams Governance and Life Cycle Management	347
Microsoft Teams Identity and Access Management	348
Managing Information Protection Using Data Loss Prevention	354
Creating and Managing eDiscovery for Teams	362
Data Governance and Retention in Teams.....	364
Managing Internal Risk Through Information Barrier in Teams.....	370
Creating and Managing Office 365 Group Classification	373
Creating and Managing Office 365 Group Expiration Policy That Applies to Associated Content.....	376
Creating and Managing Office 365 Groups Naming Policy Applicable to Teams	380
Summary.....	385

- Chapter 6: Migration from Skype for Business (Lync) On-Premises and Online to Microsoft Teams 387**
 - Getting Ready for Microsoft Teams 387
 - Understanding the Migration Path and Coexistence Modes 389
 - Planning and Implementing a Successful Upgrade from Skype for Business to Teams..... 391
 - Skype for Business to Microsoft Teams Upgrade Mode 392
 - Teams Upgrade Coexistence Modes Are Available as Deployment Path 394
 - Teams Side-by-Side (Islands) Mode 395
 - Migrating Users from Skype for Business Online (CCE) and On-Premises to Microsoft Teams (Teams Only Mode) 403
 - User Migration from Skype for Business Online to Teams Only Mode with or without Calling Plan..... 404
 - User Migration from Skype for Business Online Users with Cloud Connector Edition..... 406
 - User Migration from Skype for Business On-Premises with Enterprise Voice to Teams Only with Direct Routing 407
 - Teams Only Experience for End Users 411
 - What Happens to Skype for Business During the Upgrade?..... 412
 - Client Experiences Between Skype for Business and Teams 413
 - Migration Tips and Tools 416
 - Teams Meeting Migration Service Tool..... 416
 - Tips for User Migration 418
 - Skype for Business to Teams User Migration Tool 418
 - Summary..... 423
- Chapter 7: Microsoft Teams Troubleshooting Approaches 425**
 - Microsoft Teams Foundation Details That Help in Troubleshooting..... 425
 - Teams Features and URL Dependency 426
 - Why Do I Care About Network Traces in Teams? 427
 - Microsoft Teams Sign-in Issues 428
 - Microsoft Teams Administrative Roles..... 428
 - How Teams Authentication Works 429
 - Teams Sign-in Issues and Corresponding Error Codes..... 429
 - Approaching Teams Issues 432

Collecting Teams Client Logs.....	433
Microsoft Teams Client-Side Troubleshooting.....	436
Teams Client-Side Troubleshooting	436
Teams Client Connectivity Troubleshooting	442
Teams Audio and Video Call Quality Issue Troubleshooting	442
Teams Audio and Video Call Quality Issues and Dependency	443
How Teams Audio and Video Calls Work.....	446
Teams Phone System (PSTN) Call Troubleshooting.....	451
Customizing Call Features in Teams Client.....	451
Phone Dial-Pad Is Missing in Teams.....	453
Troubleshooting Call Failures with Call Analytics	453
Unable to Connect to Voicemail in Teams.....	454
If You Are Unable to Connect to Exchange, Then Teams and Outlook Connectivity Breaks.....	454
Restoring a Deleted Channel	455
Available Tools for Effective Troubleshooting	455
Verifying Teams Service Health Using Health Tool.....	455
Checking Teams Service Health	457
Microsoft Teams Network Assessment Tool	458
SIP Tester.....	460
Summary.....	461
Chapter 8: Take Your Learning to the Next Level	463
Planning and Preparing for the Managing Microsoft Teams Exam	464
Understanding the Exam Structure for Managing Microsoft Teams (MS-700)	464
Exam Summary	465
Additional Resources for Exam Preparation.....	483
Summary.....	484
Glossary	485
References	487
Index.....	495

About the Author



Balu N. Ilag is a Microsoft Certified Trainer (MCT), Microsoft 365 Certified Teams Administrator Associate, and Microsoft Certified Solutions Expert (MCSE) for communication and productivity. He has written several blog posts on unified communication and collaboration technologies including subjects ranging from a how-to guide to best practices and troubleshooting.

He is currently working as an Office 365 and communication and collaboration specialist. He has more than 13 years of experience in messaging, telecom, and unified communications and collaboration, focused on Microsoft Teams and Microsoft Office 365 collaboration. His role is a combination of product administration, product development, and strategic guidance for enterprise customers.

About the Technical Reviewer



Vikas Sukhija has more than a decade of IT infrastructure experience. He is certified and has worked on various Microsoft and related technologies.

He has been awarded the Microsoft Most Valuable Professional title three times in Cloud and Datacenter Management (2015, 2016, 2017-18) and once in the Office 365 category (2019-20). With his experience in messaging and collaboration technologies, he has assisted clients in migrating from one messaging platform to another.

He has used PowerShell for automation of various tasks and has created self-service solutions for users. He has been recognized many times by clients for reducing costs through automation. He is currently playing a key role with various large clients in implementation and adoption of Office 365.

Vikas is the owner and author of a blog at <http://TechWizard.cloud>, <http://SysCloudPro.com> and the Facebook page at <https://www.facebook.com/TechWizard.cloud>.

Acknowledgments

Thank you to all the individuals with whom I have had the opportunity to interact for educating me. My colleagues and friend have always believed in me, and I thank them for being so kind.

Thank you to Microsoft for making such a good product and making product information available so individuals like me can make use of it.

I especially want to say thank you to my MOHO friends, who are always there to help in any way.

Introduction

Teamwork is essential in the digital transformation of any organization to a modern workplace. Through teamwork, places can pull together using working tools and well-channeled communication methods. However, even as the team plans to work together, there are challenges in team collaboration. There are several approaches Microsoft Teams uses to ensure it can solve communication and collaboration challenges. For instance, Microsoft Teams facilitates proper communication and collaboration in an organization. Using Teams, users will be able to communicate through voice, video, real-time chat, content sharing, and meetings with dial-in and desktop sharing. The applications in Microsoft Office 365, such as Microsoft Office, Word, Excel, PowerPoint, Outlook, Planner, Task Management, OneNote, Exchange, and SharePoint, are also integrated with Teams to bring together work tools and resources.

Microsoft Teams is a vast product, and it does have several features that make administration challenging. This book is a reference guide that provides solutions, tips, and workarounds for all you need to plan, customize, implement, and operate Microsoft Teams in any environment. This book on Microsoft Teams unified communication and collaboration technology is devoted to a Teams workload, administration, tools, and technique during the various deployment and migration phases of Teams.

This completely rewritten book thoroughly reviews the administration tools and capabilities available in the latest versions of Microsoft Teams, and adds extensive new coverage of Teams services, Phone System Direct Routing, calling, Meeting, and most important, problem-solving approaches. Learn how professionals solve unified communication and collaboration challenges by architecting the Teams experience effectively.

Who Is This Book For?

This book is for everyone who uses or supports Microsoft Teams. You will learn about the user experience effective Teams management, requirements, and essential considerations for deploying Teams as part of a Microsoft 365 installation. You'll also learn about Teams governance policies, such as expiration, retention, and archiving [73].

INTRODUCTION

This book alone won't transform you into a Teams administrator or support engineer or consultant any more than a few swimming lessons will turn you into a world-class swimmer. However, if you are a helpdesk employee, Teams administrator, support engineer, unified communication (UC) consultant, or anyone else who uses Microsoft Teams daily or occasionally, this book covers basic and advanced-level Teams administration so that you can respond to your end users' questions, solve their Teams-related support queries, implement Teams meeting and messaging policies, understand ideal management, and undertake planning and preparation of your environment for Teams migration from Skype for Business. Most important, you can systematize, design, and implement responsibilities such as the following:

- Understand the Teams architecture and Teams datastore location.
- Prepare your organization network to support the Teams workload.
- Implement quality of services for Teams inbound and outbound traffic.
- Implement and configure a virtual private network (VPN) split tunnel for Teams to provide an optimal experience for VPN users.
- Configure and customize messaging, meeting, live event, and Teams governance policies.
- Set up Teams organization-wide policies for guest access and external access.
- Troubleshoot Teams sign-in, connection, and call quality issues.
- Prepare and plan for Managing Microsoft Teams certification.

These tasks are essential for the successful management and deployment of Microsoft Teams.

What Is the Teams Administrator Role?

Microsoft Teams administrator is a new role Microsoft introduced based on extensive market research [72]. Many organizations have started thinking about a Teams administrator role because Teams is a comprehensive product that requires multitechnology knowledge including, but not limited to, Office 365, Teams services, Web service, Azure Active Directory (AAD), basic networking knowledge, public switched telephone network (PSTN) and phone system knowledge, and more.

The Microsoft Teams administrator configures, deploys, and manages Office 365 workloads for Microsoft Teams that focus on efficient and effective collaboration and communication in an enterprise environment. The Teams administrator must be able to plan, deploy, and manage all Teams features. The Teams administrator would also be responsible for upgrading from Skype for Business to Teams and must be familiar with telephony integration and Teams Direct Routing using Session Border Controller (SBC), and phone system calling plans and audio (dial-in) conferencing.

The Teams administrator collaborates with telephone engineers to integrate advanced voice features into Microsoft Teams, including but not limited to configuring Teams Direct Routing using SBC, integrating telephony, phone number (DID) porting, voice gateway for analog devices, and so on. The Teams administrator might work with other workload administrator roles, including those responsible for security and compliance, messaging, networking, identity, and devices [72].

About This Book

This book provides you a learning path including how you can use Teams to facilitate teamwork and communication within your organization, whether you are using existing unified communication (e.g., Skype for Business, formerly known as Lync) or new online deployment. It also covers Teams on a wide range of devices, from desktops to tablets to phones, taking advantage of all the rich functionality of Office 365 applications. You'll gain an understanding of how Teams provides a comprehensive and flexible environment for collaboration across applications and devices.

Here is a brief rundown of what you will learn about Teams in each of the chapters.

Chapter 1, “Microsoft Teams Overview,” introduces Microsoft Teams, including Teams architecture, necessary details on what teams and channels are, and detailed information on Microsoft Stream and Microsoft Live events. In addition, you will learn about Teams voice and video calls and meetings with a phone system overview and an overview of Teams licensing.

Chapter 2, “Managing and Controlling Microsoft Teams,” covers the complete administration experience using Teams admin center. This includes topics such as Teams authentication, managing and configuring multifactor authentication and conditional access for Teams, managing teams and channels, deploying and managing the Teams client, configuring and managing Live event and Microsoft Stream policies, and managing Teams using the Microsoft Teams admin center through different administration tools.

INTRODUCTION

Chapter 3, “Organization Readiness for Microsoft Teams,” provides detailed information on the network assessment and bandwidth planning for Teams, deploying and managing quality of service (QoS), and deploying VPN split tunnel for Microsoft Teams media traffic.

Chapter 4, “Teams Audio Conferencing and Phone System Management,” covers Teams meeting planning and Teams audio conferencing implementation, as well as Teams phone planning and preparation with configuration details on Direct Routing, Calling Plans, and additional Phone System features including call queues and auto attendant. Finally, this chapter covers voice routing policies, including dial plan, voice routing policies, and call routing.

Chapter 5, “Microsoft Teams Governance and Life Cycle Management,” includes user provisioning for Microsoft Teams, Teams governance, life cycle management, Teams identity management (including the conditional access policy), managing information protection using Data Loss Prevention (DLP), Creating and managing eDiscovery for Teams, managing data governance and retention in Teams, managing internal risk through Information Barrier (IB) in teams, creating and managing Office 365 Group classification for Teams and Outlook, creating and managing Office 365 Group expiration policy for Teams, and creating and managing Office 365 Groups naming policy for Teams.

Chapter 6, “Migration from Skype for Business (Lync) On-Prem and Online to Microsoft Teams,” covers premigration readiness, understanding the migration path and coexistence modes, migrating users from Skype for Business Online (CCE) and On-Premises to Microsoft Teams, Teams-only experience for end users, and migration tips and tools.

Chapter 7, “Microsoft Teams Troubleshooting Approaches,” provides comprehensive coverage on troubleshooting Teams access, understanding the Teams foundation for troubleshooting, Microsoft Teams sign-in issues, Microsoft Teams client-side troubleshooting, Teams audio and video call quality troubleshooting, Teams Phone System (PSTN) call troubleshooting, and the available tools for effective troubleshooting.

Chapter 8, “Take Your Learning to the Next Level with Certification,” is included specifically for providing detailed information on planning and preparation for the Managing Microsoft Teams exam with three sections: Section 1, “Plan and Configure a Microsoft Teams Environment,” Section 2, “Manage Chat, Calling, and Meetings,” and Section 3, “Manage Teams and App Policies.” At the end, the chapter includes additional resources for exam preparation.

Downloading Microsoft Teams

The Microsoft Teams client application is available for all devices, including desktop (Windows and macOS), iOS, and Android, and even a web client for the user who does not have dedicated machines. You can access Teams simply using the browser link <https://teams.microsoft.com>. To access Teams, simply enter this URL in your browser and provide your organization or school login credentials. For example, `balu@bloguc.com` is my login account, and my password will allow me to log in to Teams. It will also allow you to download the client application, or you can continue using the web application.

If you are an individual who is not affiliated with any organization or school and wants to try Microsoft Teams, then simply browse to <https://products.office.com/en-us/microsoft-teams/free> (see Figure 1). There you can register and you can the free version of Teams, which does have limited functionality.

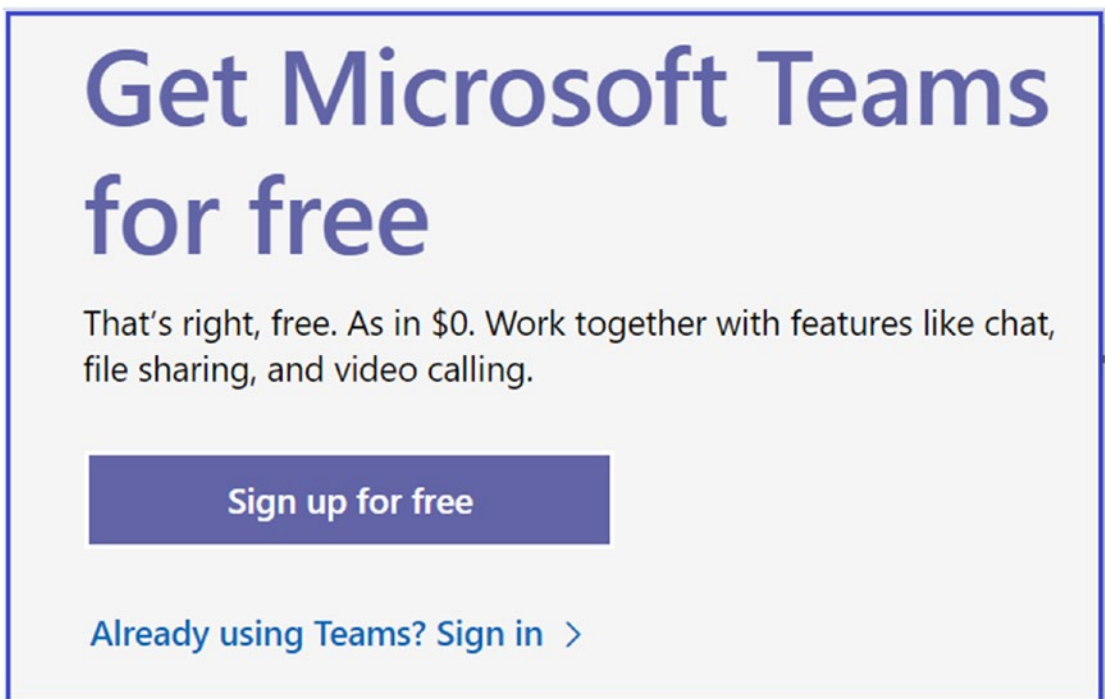
The image shows a promotional banner for Microsoft Teams. At the top, the text reads "Get Microsoft Teams for free" in a large, bold, blue font. Below this, a smaller black font text says "That's right, free. As in \$0. Work together with features like chat, file sharing, and video calling." In the center, there is a prominent blue button with the white text "Sign up for free". At the bottom of the banner, there is a link in blue text that says "Already using Teams? Sign in >". The entire banner is enclosed in a thin blue border.

Figure 1. Teams free version

Finding Help in the Teams App

Working with the Microsoft Teams new user interface, you might encounter some difficulties, such as how to change the Teams theme, how to make an announcement in Teams, how to schedule a Teams meeting, and so on. Microsoft has provided all necessary functionality help in the Help app that is located at the bottom right corner of the screen. Figure 2 shows the Help app menu opened by clicking the icon. This menu allows you to browse topics.

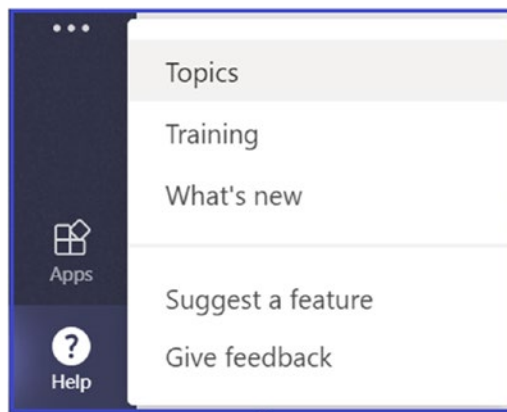


Figure 2. Teams Help app menu

Book FAQs

Will This Book Help Me Pass the Managing Microsoft Teams Certification Exam?

Yes and no. This book provides extensive guidance and real-world experience in managing and administering Microsoft Teams capability, along with customizing Teams, organization policies, and settings. In addition, this book has a dedicated Chapter 8 that covers Managing Microsoft Teams certification topics and exam preparation. However, without your individual efforts, this book on its own cannot guarantee that you will pass the Managing Microsoft Teams certification exam.

Does This Book Help Me in Succeeding on the Teams Administration Interview?

Yes, this book will assist you by offering guidance on Teams administration and management. However, without your own efforts, this book alone cannot guarantee that you will succeed on the Teams administration interview.

Can I Find Every Answer in This Book? How Can I Effectively Ask Questions?

You will find valuable administration and management details in this book and answers that you are looking for. Microsoft is adding new features and enhancing existing Teams capabilities frequently and adding admin control to manage these features in the Teams admin center and via PowerShell command; it is therefore impossible to cover upcoming Teams capabilities and controls. If you cannot find the answer that you are looking for, then visit our blog site (<https://bloguc.com>) to learn about new Teams features and administration details. Additionally, you can search online specifically in the Microsoft documentation (<https://docs.microsoft.com/en-us/>) or in the Tech community (<https://techcommunity.microsoft.com>). Remember, though, that there are smart ways to ask Microsoft Teams administration-related questions that help others help you. Be sure to read the Frequently Asked Questions sections on Knowledge Base websites and use the proper method of posting questions.

When asking Teams administration questions in any technical forum, do the following:

- Describe what you are trying to do in Teams, not just what you did. This lets your helper know if you are on the wrong path.
- I would recommend typing the exact error message or providing an error screenshot, if any, that you are getting, which allows the assistant to provide a precise answer.
- Specify what you have already tried to solve your problem. This tells the helper you have already put some effort into figuring out the Teams issue.

INTRODUCTION

- Sometimes the issue is related to the Teams client application version or operating system that you are using, so providing the client version and operating system version details helps the assistant to isolate the problem.
- Most Microsoft Teams call quality issues are related to the network, and it is always helpful to check your network setting and connectivity before asking the question over a support forum.
- It is not good practice to share organization and customer details. Always hide customer or user details before sharing a query in an online support forum.

Getting Ready

Microsoft Teams is a significant product that involves multiple services with their dependencies on network infrastructure and operating systems. Therefore, to be successful in Teams deployment or the support field, you must learn Microsoft Office 365 services and some necessary network details that will help you on the Teams journey.

We are helping people to learn unified communication and collaboration technologies, specifically the Microsoft unified communication and collaboration stack through writing UC and collaboration blog posts on various Teams user and administration topics. My blog posts are available at <https://bloguc.com>, and you can contact me with any questions or feedback at balasaheb.ilag@hotmail.com or bilag@bloguc.com.

If you could spare a few minutes to let us know what we are getting right and what we can improve, your feedback is always welcome.

This book will allow you to learn Microsoft Teams management and administration and can take you from zero knowledge to professional. However, you might have a question that goes beyond its scope. Remember that asking about a practical problem and knowing how to find answers are essential instruments on your Teams learning journey.

Let's get started!

CHAPTER 1

Microsoft Teams Overview

These days, communication needs are frequently changing because of the modern workforce, which has evolved to be more focused on team contributions than those of an individual. As technology creates remote and global teams, all users must be able to connect. Microsoft Teams provides all that the modern workforce requires. Teams is a single product that also offers a complete meeting solution, supporting sharing, voice, and video conferencing, allowing users to meet from anywhere. Users can use Teams for all types of meetings—spontaneous or scheduled, formal or informal—with internal and external participants.

Microsoft Teams is a unified communication and collaboration tool build on a cloud platform that combines various services for collaboration, such as chat, meetings, calling, and files. Teams is tightly integrated with Office 365 and combines multiple workloads into a unified communication and collaboration system. Teams also offers integration capabilities for additional tools and third-party applications.

This chapter covers several introductory topics to get you started with Teams. At the end of this chapter, you will be able to describe:

- What Microsoft Teams is and what it is used for.
- Microsoft Teams architecture and different components involved.
- How Microsoft Teams stores data and interacts with SharePoint Online and OneDrive for Business.
- Where Teams stores chat conversations and how Teams interacts with Exchange.
- Live events and their architecture.
- What Microsoft Stream is used for and its architecture.

- Teams Phone System overview and voice communication capabilities.
- Teams licensing requirements and add-on licenses.
- Teams integration with Office 365 and third-party applications.

What Is Microsoft Teams?

Microsoft Teams is a center for teamwork, which brings chat, meeting, calling, content, office 365 application, and the third party and custom applications all in one place [1]. A definition of *team* that resonates better with Teams is “a collection of people, content, and tools surrounding different projects and outcomes within an organization.” According to Microsoft, the teams formal definition is a collection of people, content, and tools surrounding different projects and outcomes within an organization.

Teams is a single product that provides extensive capabilities, starting with a conversation platform that allows team members to communicate via voice and video calls, with content sharing and application integration opportunities that teams and team members require to be successful in their technical journey.

Microsoft Teams Architecture

Microsoft Teams brings together Office 365 services and intelligent communications to provide a single platform. Before using Microsoft Teams, you, as an administrator, support person, or even end user, must understand the design and how Teams services work together to provide a unified experience.

Understanding the Microsoft Teams architecture is crucial because without knowing the Teams architecture building blocks and their functionality, you as an admin cannot manage teams or answer user questions. One of the important questions users often ask is, “Where are my Teams data stores?” In Microsoft Teams, each feature stores data in different services. Hence, it is also essential to understand Teams data storage. The word *architecture* came from the Latin *architectura*, which means building boxes [2].

Teams Architecture Overview

It is essential to understand how Teams was architected and what is happening behind the scenes. As Figure 1-1 shows, from an architecture perspective, Microsoft Teams brings together Office 365 services and intelligent communications (intelligent communications is the Skype next-generation service). Microsoft 365 Core Services such as Exchange Online, SharePoint, and OneNote; Office 365 apps; and the intelligent communication cloud are the components of the architecture that enable all communication capabilities including persistent chat, meetings, and audio and video calls. Teams services are the services that the Microsoft engineering team built to create Microsoft Teams. They orchestrate the layer that brings together all the other pieces; for example, attaching an Office 365 Group to a team created for easy membership management.

This is important because whenever someone creates a team, two things happen on the back end. First, creating new team creates an Office 365 Group for membership management (that's how Teams manages membership); second, Teams also creates a SharePoint Team site for file sharing. This means every team has an Office 365 Group as well as a SharePoint team site. All these features build on the same scalable Azure infrastructure that Microsoft used in Teams. On the top rest the Teams clients, which are available for all platforms, such as the Teams Web app, Teams desktop client (Windows and macOS), Teams Mobile app (iOS and Android), and Teams Linux client.

In many cases, the Teams client not only sits on top of the Teams layer, but it is also more efficient because it directly talks to the Office 365 services as well.

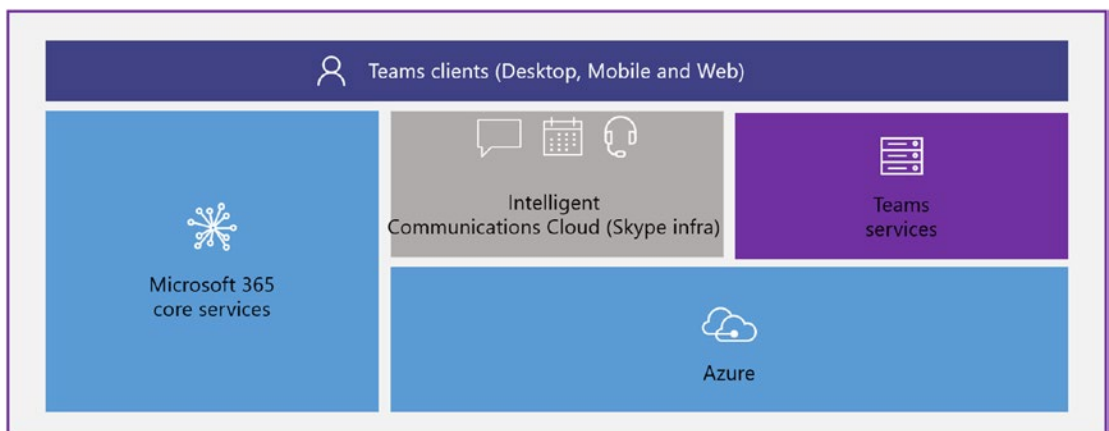


Figure 1-1. Teams high-level architecture [4a, 7a]

To help you in the deployment of a Teams client in your organization, Microsoft has added Microsoft Teams client to Microsoft 365 Pro. In addition, Microsoft Teams has a semiannual update channel.

What Is the Intelligent Communications Cloud?

You might be wondering what the intelligent communications cloud is and what it consists of. The Intelligent communications cloud was formerly known as the Skype next-generation service; it is where the messaging, calling, and meeting services, people, configuration, and identity service reside (see Figure 1-2). These represent the next-generation evolution of Skype services that Teams uses for messaging and voice over IP (VoIP) calling. The intelligent communications cloud also contains the PSTN telephone network integration system, and that is also used for the Skype for Business Online stack. Another critical service is a unified presence for Teams and Skype for Business Online.

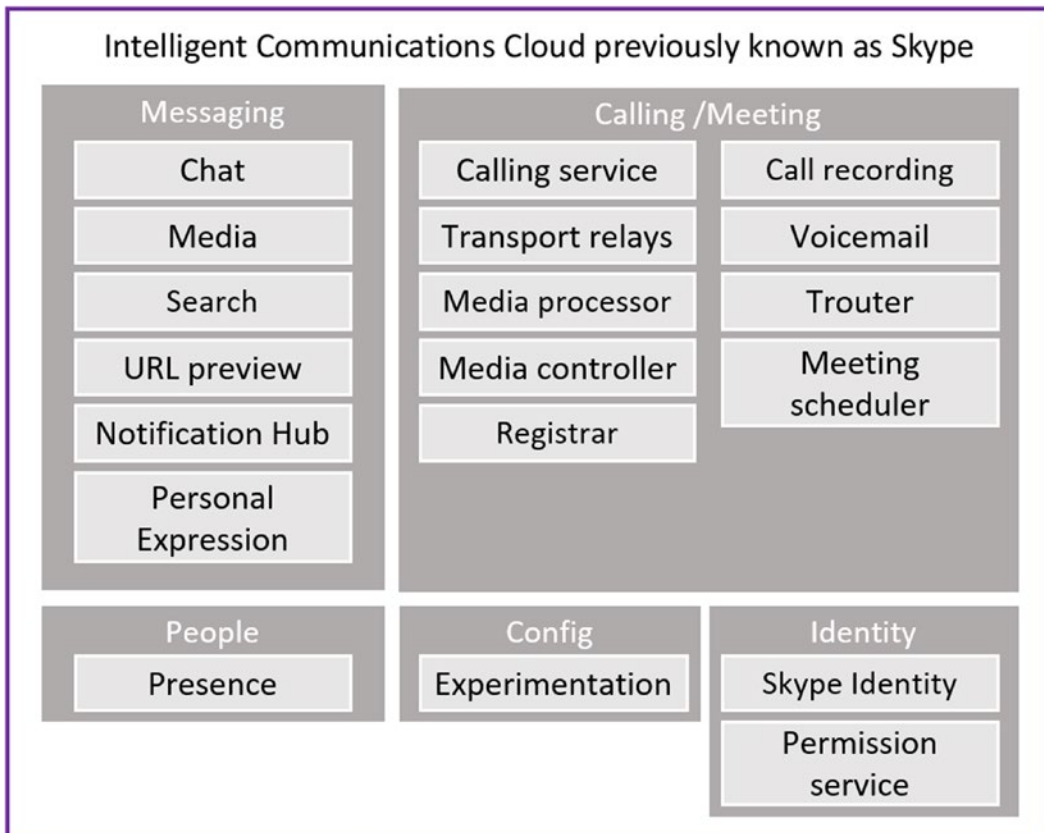


Figure 1-2. Microsoft Teams next-generation services [4a, 7a]

Note There is no unified presence between Microsoft Teams and Skype for Business On-Premise.

The messaging stack handles messaging as well as media, which means images attached in chat go to blob storage. This stack also takes care of search functions, URL preview (when a user puts a URL in Teams chat it shows a preview from the URL preview service). Notifications for tracking activity that happens in the team and personal expression services for emojis and stickers are handled in the messaging stack.

The calling and meeting stack includes call recording, calling, voice mail, Trouter, and meeting scheduler services.

The presence server gives users' presence or availability information. The configuration service for experimentation and Identity for Skype (consumer) identity have different tokens than the Active Directory token for authorization and permission services.

Microsoft Office 365 Services Used by Teams

Figure 1-3 shows the Office 365 components. Applications include OneNote, PowerApps, Planner, PowerPoint, Word, and Excel. Platform services include Exchange for email and calendars in Teams (this is the same as Outlook calendar, as Teams uses graphs to retrieve the calendar). Additional features include Modern Groups, also known as Office 365 Groups, SharePoint for content collaboration, Stream for voice recording, OneDrive for Business for file sharing, and Information Protection, which provides a shield for these services. The final component is Power BI for data analytics.

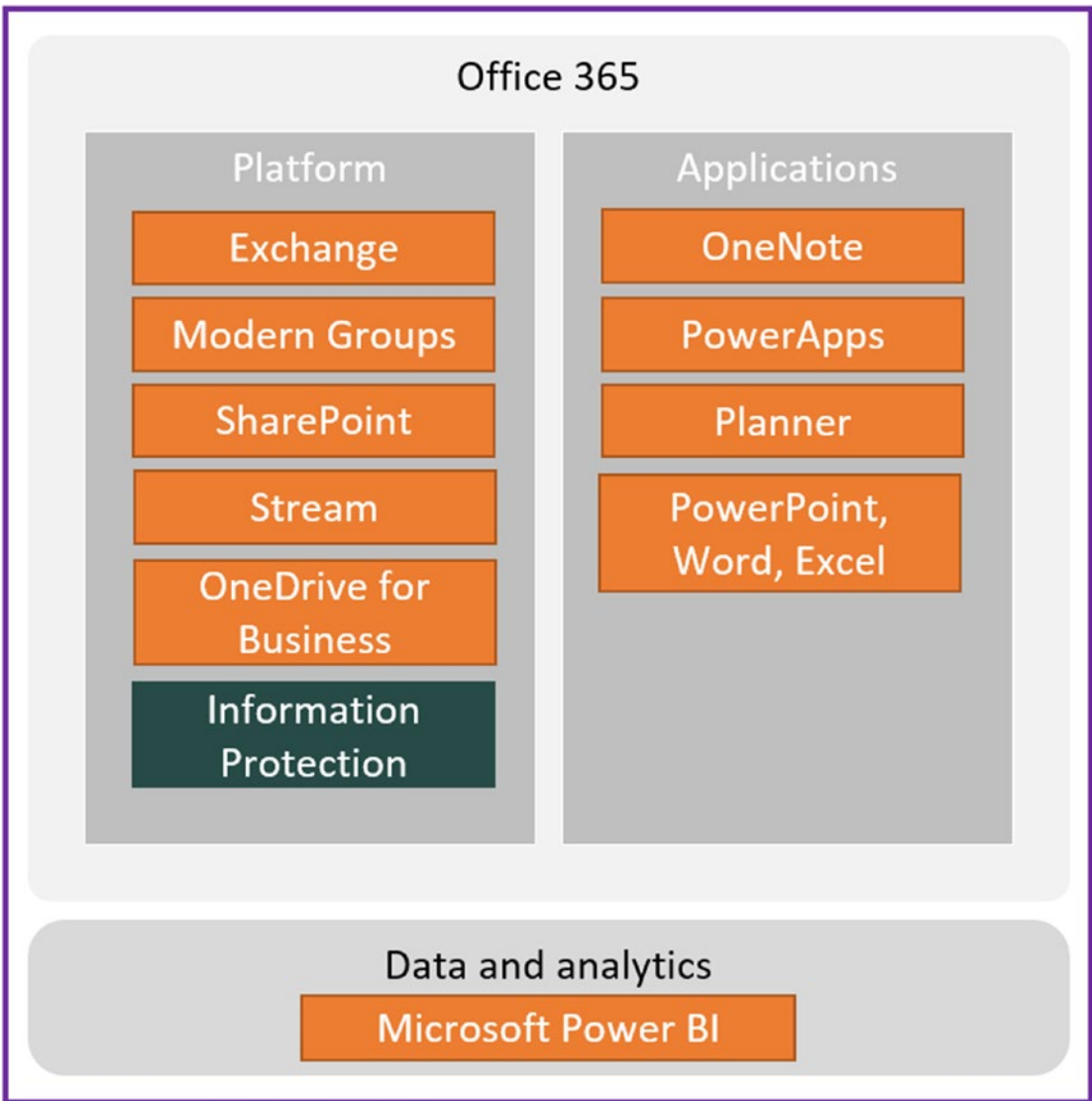


Figure 1-3. Office 365 services and Teams [4a]

Office 365 provides a great set of services and applications, but there is nothing that synthesizes all of the functionalities in one place as one application. Microsoft envisioned Teams as that application that makes the whole greater than the sum of its parts. That’s why Microsoft built Teams this way, to be the hub of Office 365.

Microsoft Teams Capabilities and Their Data Storage Locations

Those supporting Teams users frequently get asked by users where their Teams data is stored, including conversations (chat), files that users shared, images, and others. Teams chat is persistent, which means it is stored entirely, and it uses its own storage. Group chat and one-to-one chat is stored in Cosmos DB, and channel conversations are stored in Cosmos DB as well [7a]. Teams also keeps a copy of all chat messages in Exchange, mainly to enable information protection.

If users have a one-to-one chat or group chat, Teams keeps a copy of that chat in the mailbox of the individuals who are part of that chat. If you chat in channel teams, Teams keeps a copy of that chat in the mailbox of the Office 365 Group that is attached to that team.

Specific to files, Teams leverages OneDrive for Business and SharePoint for file storing. There are two scenarios shown in Figure 1-4. First, a file shared with one-to-one chat is stored on OneDrive for Business and permission is automatically granted by Teams for users who need access. Another scenario is when a file is shared between channels. In this case, Teams will upload that file to the SharePoint team site that is created when that team is created and the file permission is automatically granted to every member of that team. This is important for content collaboration [7a].

Voicemail is another critical feature that most of the enterprise users utilize. Voicemail is stored in the Exchange mailbox of the user who receives the voicemail, similar to Skype for Business. Calendars and Teams contacts are also stored in Exchange. Calendar is stored in an Exchange unified group mailbox that is created with the team and user's Calendar stores in an individual mailbox.

Where are users' meeting recordings stored? Whenever a user records a meeting it is first stored in the same media storage where images are stored. The recording is then encoded and made available on Microsoft Stream for content collaboration. Within 24 hours, Teams purges the recording from media store to Microsoft Stream so that users can share their meeting recordings with others.

The Teams telemetry is stored in Microsoft Data warehouse without any customer content such as email address and contact numbers.

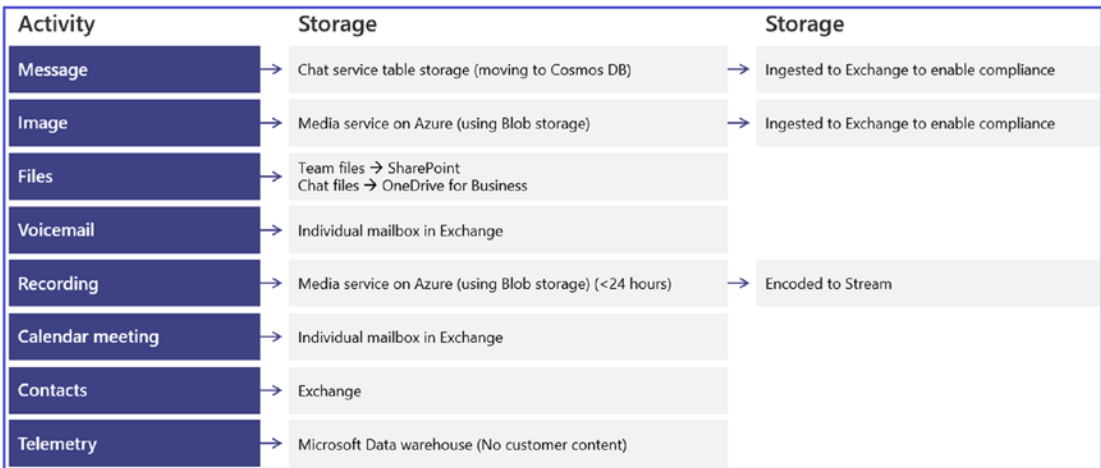


Figure 1-4. Teams activity and data storage locations [4a, 7a] [4a]

Note Data in Teams resides in the geographic region associated with your Office 365 tenant. Currently, Microsoft Teams supports Australia, Canada, France, India, Japan, South Africa, South Korea, United Kingdom, Americas, APAC, and EMEA regions.

Now that you understand how many components are involved in Teams architecture, the next important question comes from the technical community: How does Microsoft Teams intermingle with Office 365 technologies?

Teams delivers multiple functionalities, including persistent chat, online meetings, voice and video calls, calendar, content sharing, and many more. All these features come from underlying technologies, but as an admin, you must know how this technology interaction works. When a user creates a team, on the back end it creates a new Office 365 Group, SharePoint Online site, and document library to store team files. Exchange Online shares a mailbox with the Calendar, and a OneNote notebook is automatically provisioned for the team.

Microsoft Teams Logical Architecture

In Figure 1-1, you saw the different components of Teams and how they communicate with each other. Figure 1-5 demonstrates the logical architecture of Teams [4]. The Teams client is the interface to access Teams services in real time for communication and collaboration for teams. Teams connector provides a novel way to integrate third-party apps.

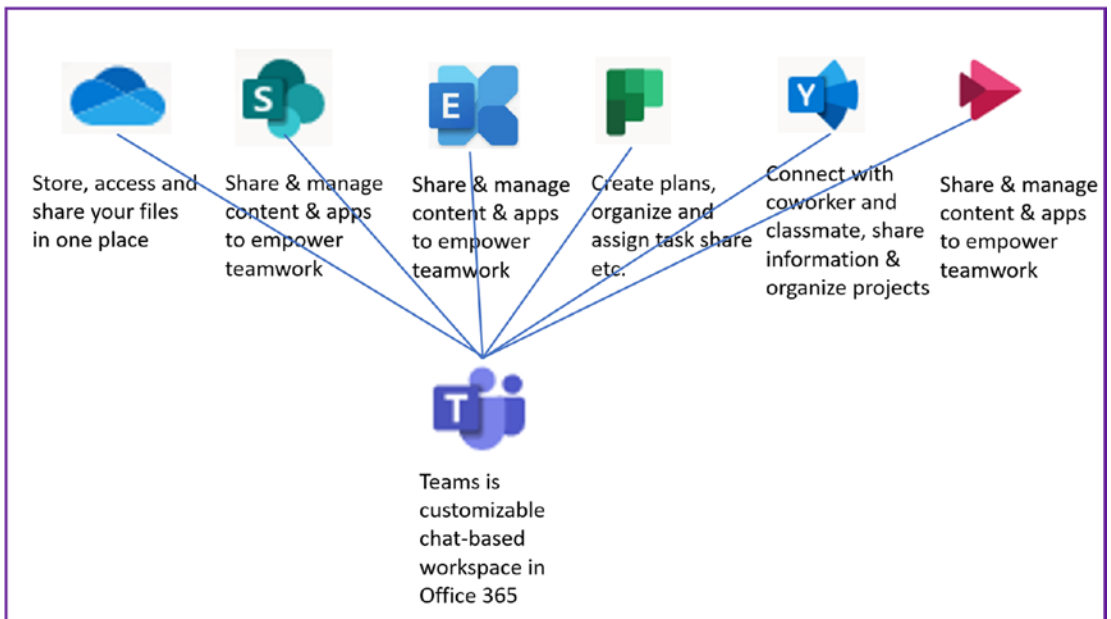


Figure 1-5. Teams interaction with underlying services [4, 4a]

Microsoft Office 365 Group and Teams are tightly integrated. For example, when a user creates a team from an existing Office 365 Group, that Group’s membership, site, mailbox, and notebook, if any, are merged in Teams. If the Office 365 Group and Teams integration breaks, then the Office Group will not materialize in Teams. That is why Office 365 and Teams are tightly integrated.

- *OneDrive for Business:* OneDrive for Business is mainly used for storing personal user documents until they are shared with others. From a Teams perspective, when a user shares a file in one-to-one chat, which is stored on OneDrive for Business, permission is automatically granted by Teams for the user who needs access.
- *SharePoint Online:* This is mainly used to store Teams files that are shared within channel and team sites. When a team creates a SharePoint site, it is automatically provisioned. Once a file is shared within a team, the access permission is automatically granted by Teams to all team members. The Teams file tab therefore directly interacts with SharePoint Team sites.

- *Exchange Online*: Every team has a group mailbox, and each team member has an individual user mailbox. Teams meetings scheduled by an individual are stored on his or her mailbox and calendar. The Teams calendar therefore directly interacts with the Exchange Online mailbox.
- *Microsoft Stream*: This service is used for creating and sharing videos securely. With Teams, all team meeting recordings are stored and shared using Stream. Also, live events (large broadcast events) are hosted in Stream, as covered later in this chapter.

Microsoft Teams Depends on Other Services

You just saw how the Teams logical architecture works with Office 365 services. Teams does have specific dependencies with other services (see Figure 1-6); for example, Teams chat features directly interact with the chat service in Office 365, one-to-one chat is stored in the user mailbox, and group chat is stored in the Teams group mailbox. Chat is therefore dependent on Exchange Online [4]. Teams files and wiki are dependent on SharePoint Team sites. Teams meetings and calls are dependent on Skype next generation calling and meeting services, meeting calendars are stored on the user's mailbox, and files (one-to-one sharing) depend on OneDrive for Business.

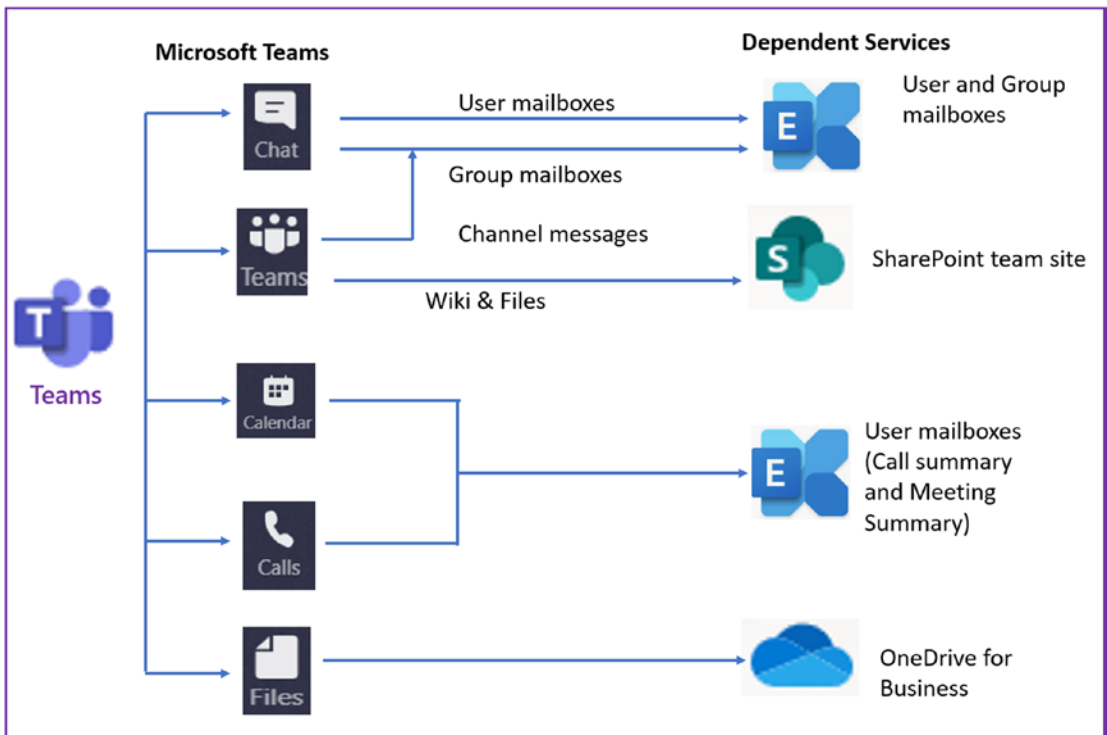


Figure 1-6. Teams dependent services [4, 4a]

Note SharePoint Online is a requirement for using OneDrive for Business. Users cannot store and share files on the channel without SharePoint Online and OneDrive for Business.

Microsoft Teams Teams and Channels

Teams

Microsoft Teams provides a tool set that a team requires to execute project tasks. When a user creates a team, he or she will be asked to choose the option to create a private team (only invited users can join) or a public team (anyone from the organization can join). As a team owner, he or she can add members and designate them as a team owner for administration. We recommend adding more than two team owners to mitigate a single point of failure. If a team has a single owner and that owner is terminated or leaves the

organization, then the team will not have an owner to administer. For this reason, having a minimum of two owners is recommended.

Note As of this writing, a team can have a maximum of 10,000 members, including private or public teams and organization-wide teams. The prior limit was 5,000 members in a team. You can refer to Chapter 8 for the complete Teams feature limitations and expiration periods.

There are three types of teams (see Figure 1-7):

- *Private team:* People need permission to join this type of team.
- *Public team:* Anyone in your organization can join this type of team.
- *Org-wide team:* Everyone in your organization automatically joins this team.

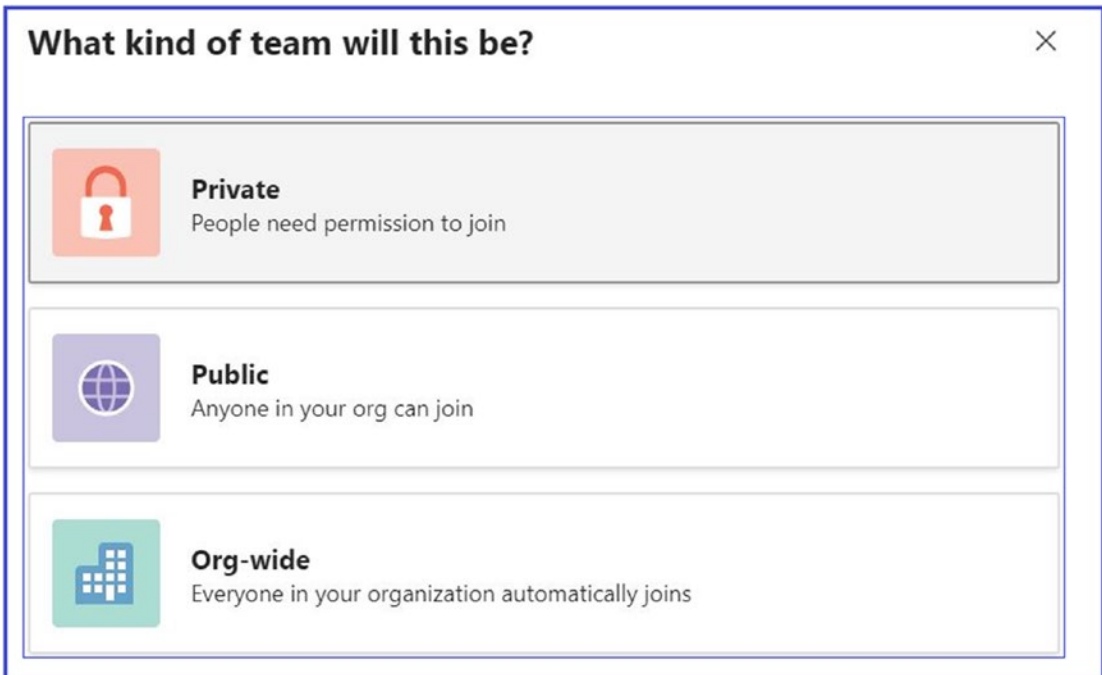


Figure 1-7. Team types

Note Regular users cannot create organization-wide teams. Only global administrators can create org-wide teams, and currently, an org-wide team is limited to organizations with no more than 5,000 users. There is also a limit of five org-wide teams per tenant.

Team creation and management are covered in Chapter 2.

Channels

A team is a collection people who gather to perform a project for their organization. That project might have multiple subtasks, so performing these individual tasks requires conversations, calls, or meetings. Each task might have separate documentation requirements. To maintain these separate tasks, Teams provide a dedicated section that is called a channel [19]. Channels are dedicated sections within a team that keep conversations organized by specific topics, tasks, or subjects. Team channels are locations where everyone on the team can openly have conversations. They are most valuable when extended with apps that include tabs, connectors, and bots that increase their value to team members.

Figure 1-8 shows the team and channel structure for the Bloguc organization. It shows three channels for each team. At this point, there is no limitation on creating channels or teams in any organization. That means your organization can have any number of teams and channels. Remember, though, that Teams management efforts increase along with the numbers of teams and channels, so as a Teams admin you must keep track of how teams and channels are used in your organization.

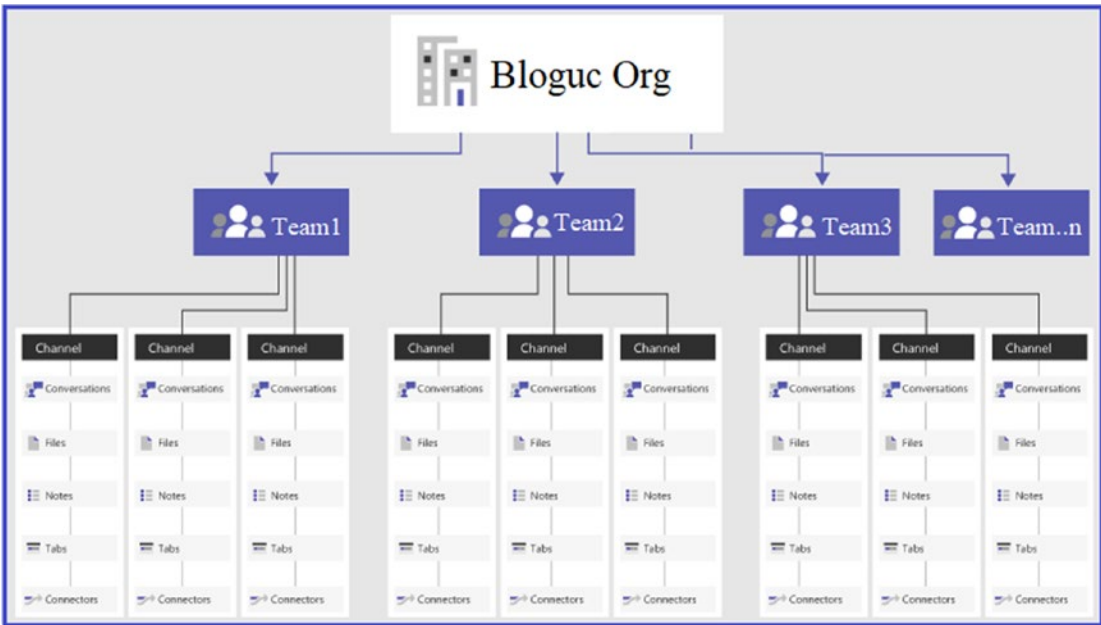


Figure 1-8. Team and channel structure

There are two types of channels (see Figure 1-9):

- *Standard channel:* The standard type of channel is accessible to everyone on the team, including team members and guest members.
- *Private channel:* Private channels are accessible only to a specific group of people within the team.

Create a channel for "UC & C Team" team

Channel name
Letters, numbers, and spaces are allowed

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

Privacy
Standard - Accessible to everyone on the team

- Standard - Accessible to everyone on the team
- Private - Accessible only to a specific group of people within the team

Figure 1-9. Team channel types and their uses

Channel use and management are covered in Chapter 2.

How Does Microsoft Teams Manage Identities?

Microsoft Teams is a cloud-only service, which means that users who access Teams must have a cloud identity. It does not mean teams require a cloud-only identity. Teams does support all identity models that are available with Office 365. Teams leverage identities stored in Azure Active Directory (Azure AD), which combines core directory services, application access management, and identity protection into a single solution.

Today Microsoft Teams supports all the identity models that are available in Office 365, including Cloud Identity, Synchronized Identity, and Federated Identity.

- *Cloud Identity model:* Using the Cloud Identity model, a user is created and managed in Office 365 and stored in Azure AD, and the password is verified by Azure AD.
- *Synchronized Identity:* Using Synchronized Identity, the user identity is managed in an on-premises server, and the accounts and password hashes are synchronized to the cloud.
- *Federated identity model:* The Federated Identity model requires a synchronized identity where the user password is verified by the on-premises or online identity provider (e.g., Active Directory Federation Services [ADFS] or Okta).

Most of the organization will use Synchronized Identity for security reasons, as users maintain their on-premises identity. They then synchronize with Azure AD through Azure AD Connect. The organization will want to maintain its own on-premises identity as the source that is synced with Azure AD. Teams then leverages the synced user identity to provide services such as enabling and assigning Teams licenses, creating a Phone System license, enabling Exchange mailboxes, assigning phone numbers, policy assignment, and so on.

The Microsoft Teams authentication process, conditional access, and multifactor authentication are covered in Chapter 2.

Tabs, Files, and Connectors in Teams

The channel tabs, files, and connectors improve the user experience and allow users to configure their frequently used applications to expedite application access.

Tabs

Tabs allow team members to access services and content in a dedicated space within a channel or in a chat. Tabs let a team work directly with tools and data and have conversations about those tools and data, all within the context of the channel or chat.

Team owners, as well as team members, can add tabs in the team channel (standard and private), channel chat, and private chat (one-to-one and group) to use Microsoft cloud applications and third-party applications in the team to manage the information that they use frequently. For example, Microsoft Planner is a useful tool to plan and

prioritize project tasks. Adding a planner as a tab allows users to access their assigned project tasks within the team.

Files

Files allow users to upload new files and share them with team members or access existing files uploaded by another team member in Teams.

Remember, in every channel, the Conversations and Files tabs are created by default. In every private chat, the Conversations, Files, Organization, and Activity tabs are created by default. Apart from the built-in tabs, the team owner and members can design and add custom tabs. Refer to the Microsoft official documentation to learn how to design a custom tab (<https://docs.microsoft.com/en-us/microsoftteams/built-in-custom-tabs>).

Microsoft Stream and Live event

Microsoft Stream is a Microsoft enterprise video solution that is part of Office 365. Customers can securely create and deliver videos to their organization. Streams support live events through Teams, Stream, and Yammer. Microsoft provides a portal to upload, share, and discover videos that can be used for things like executive communication or training and support. Microsoft Stream allows users to upload videos, search groups and videos, broadcast their live events, and categorize and organize videos. Users can also create a group and Stream that allows users to embed video in Microsoft Teams.

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

Microsoft Stream Architecture

Stream is a service, which has a front end and a set of back-end services, as shown in Figure 1-10. Users access and interact with a stream through the front end, the Stream portal that users can access by visiting [Microsoftstream.com](https://microsoftstream.com). Stream support is embedded in videos, channels, and sets of other applications, so customers who are using other applications don't have to leave their application to consume Stream

videos. Stream also supports a simplified form of embedded service. As a result, an application can call Stream to embed an endpoint to dynamically get embedded code and automatically embed videos inside of the application.

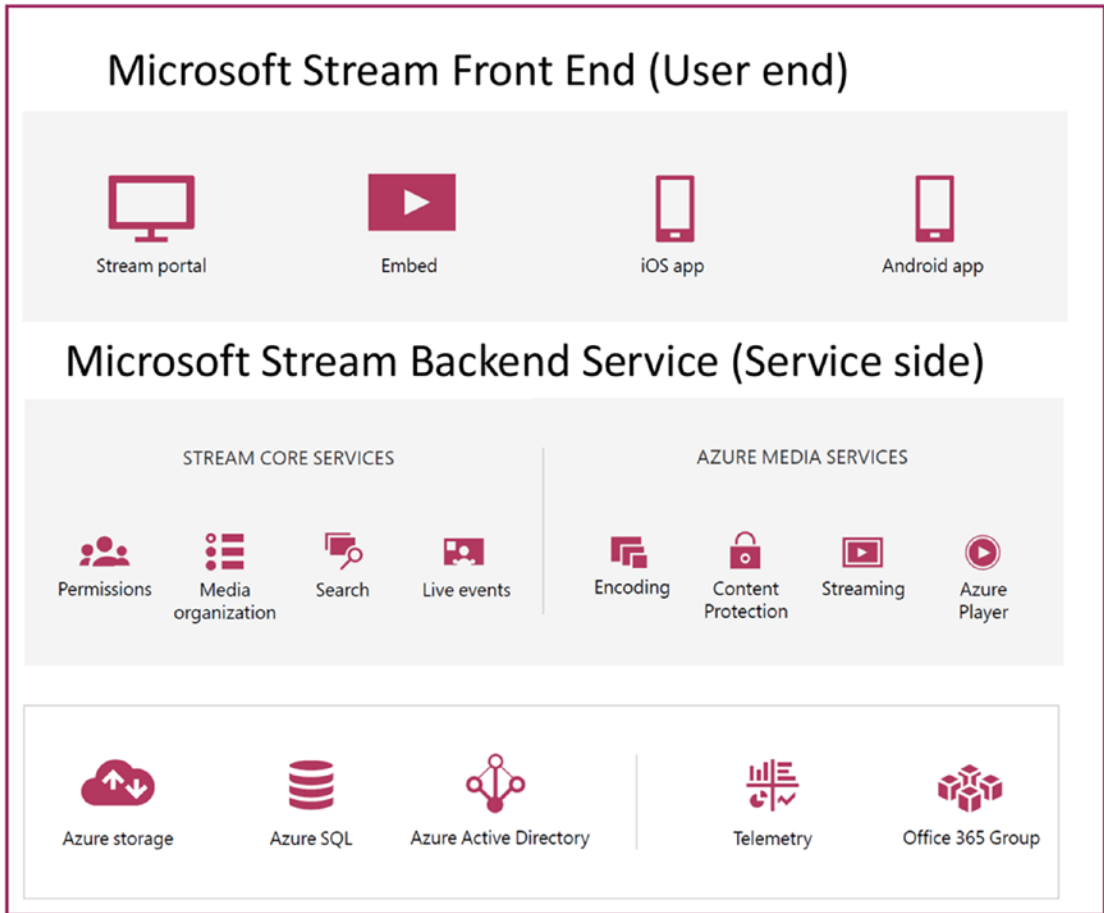


Figure 1-10. Stream architecture [68a, 69]

Stream does support iOS and Android apps that are used for consuming as well as creating content on the go using mobile apps.

Streams back-end services include Stream core services, such as permissions, media organization, search, and live events. These services use the Stream business logic. Microsoft implements a permission service that allows users to authenticate and access permitted content when they log in to the Stream portal, which allows users to authenticate and authorize to access their resources on Stream [69].

Media organization is the back-end service that allows access to groups and channels, so Stream implements Office 365 Groups and channels and this service organizes the content.

Search is another back-end service. When a user inputs keywords, that search usually takes place inside the title and description. Stream also does a deep search inside its automatically generated transcripts to find the most relevant content for users.

Stream supports live events, and all the involved logic, including live event scheduling, connection with an encoder, working with Azure Media Services to set up a channel, and getting the whole live event started. That knowledge is implemented inside the back-end service.

Microsoft Stream has dependencies on Azure Media Services. Azure Media Services is the Azure offering that does the media processing of streams through encoding. Whenever a user uploads a video to Stream (Stream supports multiple types of video formats), encoding in Azure Media Services encodes the video in different bit rates to support the various network conditions.

Content Protection dynamically encrypts the video content using Advanced Encryption Standard (AES) 120-bit encryption so that the user content is secure while streaming.

The Streaming service implements the adaptive bit rates so that irrespective of customer network conditions and media player size, streams adapt to these different conditions to provide optimal video quality.

The Microsoft Stream player is based on the Azure Media Player. In addition to that, Stream also has dependencies on other Azure services, including Azure Blob storage. That's where the video assets are stored, including video files, the thumbnail that is generated, and the transcript that is. Stream uses Azure SQL DB to store video metadata, which includes things like the title, description, permissions, and view count. Both Azure storage and SQL DB are encrypted at rest.

Azure AD is also integrated with Stream to authenticate users. Stream is also on top of Office 365 Groups, and Stream uses telemetry services to show uses and performance.

When a user logs in to the Stream portal, authentication happens first so that the user gets validated. After the login, Stream loads the front end from the nearest datacenter. For example, the Bloguc organization tenant is hosted in the United States; however, user Balu is located in India, so the front end is loaded from the datacenter that closest to user Balu, not the tenant that is in the United States. On the back end, Stream determines the back-end tenant location and loads the back-end services for the user.

Where Is My Stream Data Residing?

Microsoft Stream presently hosts data in regions including the United States, Europe, Asia Pacific, Australia, India, United Kingdom, Canada, and the U.S. Government Community Cloud (GCC). Remember, if your tenant is located in one of these regions, then your organization stream data will also be located in that region. However, if a user lives in a region not listed, then Microsoft hosts Stream data in the closest tenant region. Microsoft is planning to host Stream data in few other regions, including but not limited to China, Germany, and GCC-High/GCC-DoD (government community).

Tip To learn the data storage location in Stream, simply log in to Stream and then click About Microsoft Stream.

Microsoft Teams Live Event

Microsoft Teams provides unified communication and collaboration capabilities, including persistent chat, calling, meetings, and live events. Teams meetings are interactive meetings in which both the presenter and attendees can interact with optimal voice and video with application sharing. Teams meetings are limited to 250 attendees, though. When your organization wants to host a larger meeting, such as a broadcast events or organization-wide events with thousands of online attendees, that's where live events comes in handy. Microsoft Teams, through live events, provides an option that enables users to expand their meeting attendees by broadcasting video and meeting content online to large audiences of up to 10,000 attendees.

A live event is created for one-to-many communications (one organizer or presenter to many attendees), where the host of the event conducts the interactions. Attendees, or the audience, views the content shared by the host or presenter. The attendees can watch the live or recorded events in Yammer, Teams, and Microsoft Stream, and they can also interact with the presenters using moderated questions and answers (Q&A) or a Yammer conversation [67].

Live Event Architecture

Figure 1-11 displays the live events high-level architecture. The organizer organizes the live event in either Teams, Yammer, or Stream, depending on the production method chosen. It will be in Teams if all presenters are using the Teams client. If the production type chosen is an external app or device, the presenter can use a production app or tools like media mixer, microphones, speakers, and so on. When more professional video equipment is used and the producer is using Teams or Stream to produce live events, all this content is sent over Office 365, which uses Azure Media Services, where it goes through the Content Delivery Network (CDN) to customers.

On the left in Figure 1-11, you can see the certified third-party Enterprise Content Delivery Network (eCDN) providers (Kolletive, Hive, or Ramp) and then content viewed by all the attendees via the Teams client, Yammer, or Stream.

Note eCDN use is not mandatory; however, it will help to save your enterprise bandwidth.

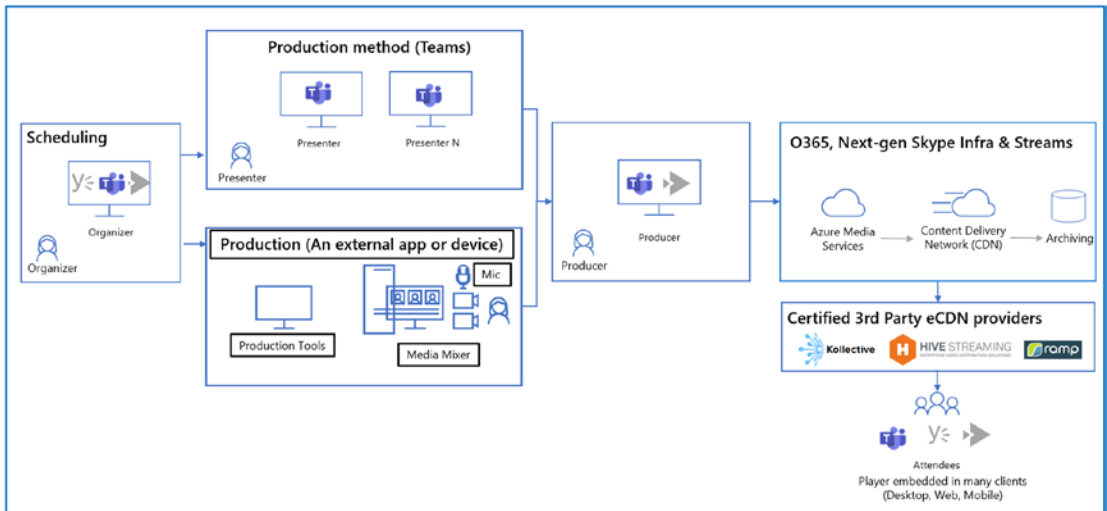


Figure 1-11. Live event architecture [67, 68]

How Do Media Flow in Live Events?

As an admin or support person, you must understand the live event architecture and how media flow in a Microsoft Teams Live event. The live events media flow is similar to a Teams meeting. If the Teams production method was chosen, all the presenters will join a native Teams meeting. It is a bit of a special Teams meeting because it has all the presenters controlling the meeting, but from a media perspective it's just a Microsoft Teams meeting. The presenters will send their audio, video, and screen sharing via Real-Time Protocol (RTP) to the meeting service, which sends the RTP traffic to Azure Media Services. If you use an external production method, however, videos provided by hardware or software encoder are sent by the Real-Time Messaging Protocol (RTMP) to Azure Media Services, all of which is basically RTP communication. Figure 1-12 shows how attendees watch Stream via Transmission Control Protocol (TCP) as a stream. Although it is not real-time communication, attendees can watch a live event as near real-time because they are viewing content created multiple seconds after it occurred (delayed); however, from a technical perspective, it is just a TCP stream that they are consuming, that is not sensitive to latency, jitter, and packet loss. If attendees have packet loss or latency network impairment, there might be delays in streaming, but they will not lose any of the content [67].

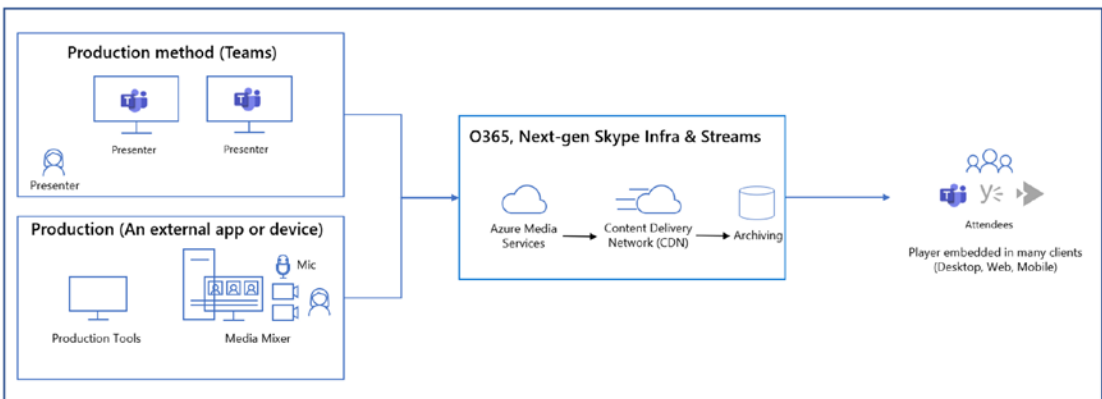


Figure 1-12. Live event media flow [67, 68]

How Does Microsoft Teams Live Events Work?

Live events are online meetings with audiences of up to thousands of concurrent viewers, where the presenter team shares audio, video, and content, and audience view that content. In live meetings, there are specific key roles that perform different activities

to run the live event successfully, and every role has different permissions assigned. Here is detailed information about each role.

- *Tenant admin:* The tenant admin has nothing to do with live event operation; however, the tenant admin can configure the live events settings for the tenant and set the right permissions.
- *Organizer:* The organizer of a live event is the person who schedules the event and ensures the event is set up with the right permissions for attendees and the event group, who will manage the event.
- *Producer:* The producer is a host of the meeting. This person is part of the event group, so he or she is invited to the event by the organizer. It is the producer's responsibility to ensure attendees have a great viewing experience by controlling the media sources that are sent to the live event. The producer actually decides whose audio and video goes live in the event.
- *Presenter:* The presenter is the person who presents audio, video, or a screen in the live event, or he or she might moderate the Q&A.
- *Attendee:* An attendee just views or watches the event live on demand, either anonymously or authenticated. Attendees can participate in the Q&A.

You can schedule live events using different options. As a user or admin, you can schedule the live event in the Teams client, Yammer, or Stream. Producer options for the live event are using the Microsoft Teams client or using the external (third-party) encoder as the source used for production methods. If you are unable to schedule a live event and get an error message that indicates you do not have a live event meeting policy assigned, contact your organization admin to allow you to schedule a live event.

How Does the Live Event Production Method Work?

You can produce a live event using two different methods, using Teams or using an external app or device.

Using the Teams Live Event

In a Teams live event, all audio, video, and content captured from a producer or presenter are joined into a Teams regular meeting. For example, presenters and the producer both join a Teams meeting and share audio, video, and content (see Figure 1-13).

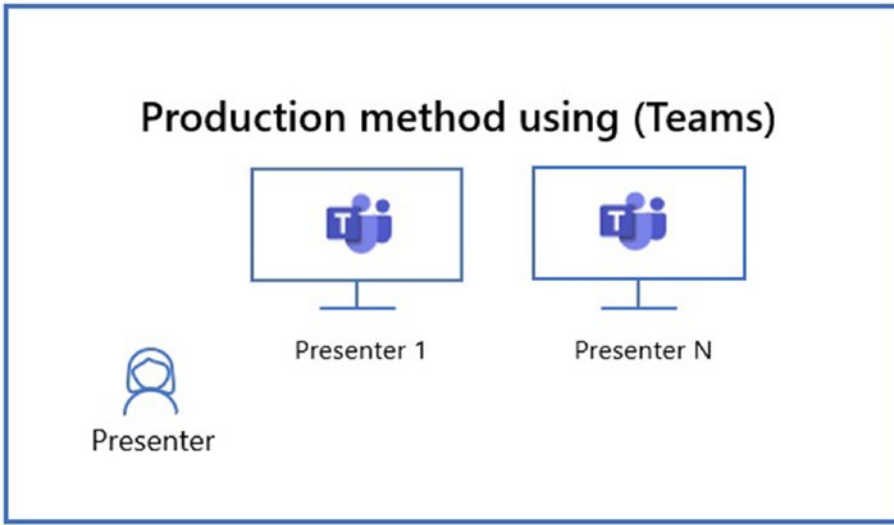


Figure 1-13. Live event production through Teams

Using an External App or Device

In an externally coded live event, audio and video come from an external hardware or software encoder (see Figure 1-14). All media comes in one stream and goes into the live event meeting, then it is broadcast to all attendees. Learn more about external encoders by visiting <https://aka.ms/teams-encoder>.

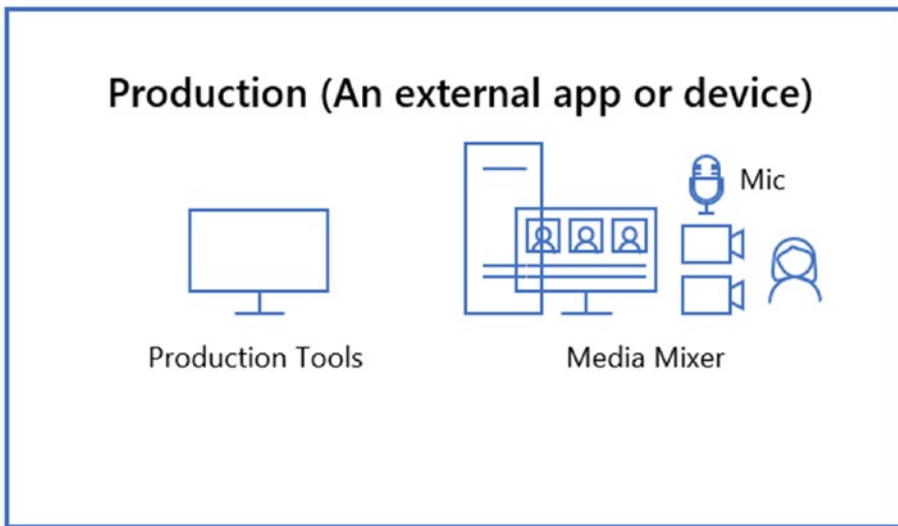


Figure 1-14. Live event production through external apps [67]

How Do I Use Live Events Effectively with Minimum Knowledge?

Live events can be scheduled quickly in teams, and users can present and produce live events from a macOS or Windows Teams client with one or more presenters, including application sharing. You can present from a Teams room system, or a presenter can join via phone dial-in to a live event using Teams Audio Conferencing. You, as a live event organizer, can control access to the public, including everyone from an organization, or specific groups or people.

Organizing a live event is very simple: Start by scheduling the event. As shown in Figure 1-15, scheduling a live event in Teams is straightforward. Just click Meeting and then choose Live event and set permissions like public, org-wide, or people and group.

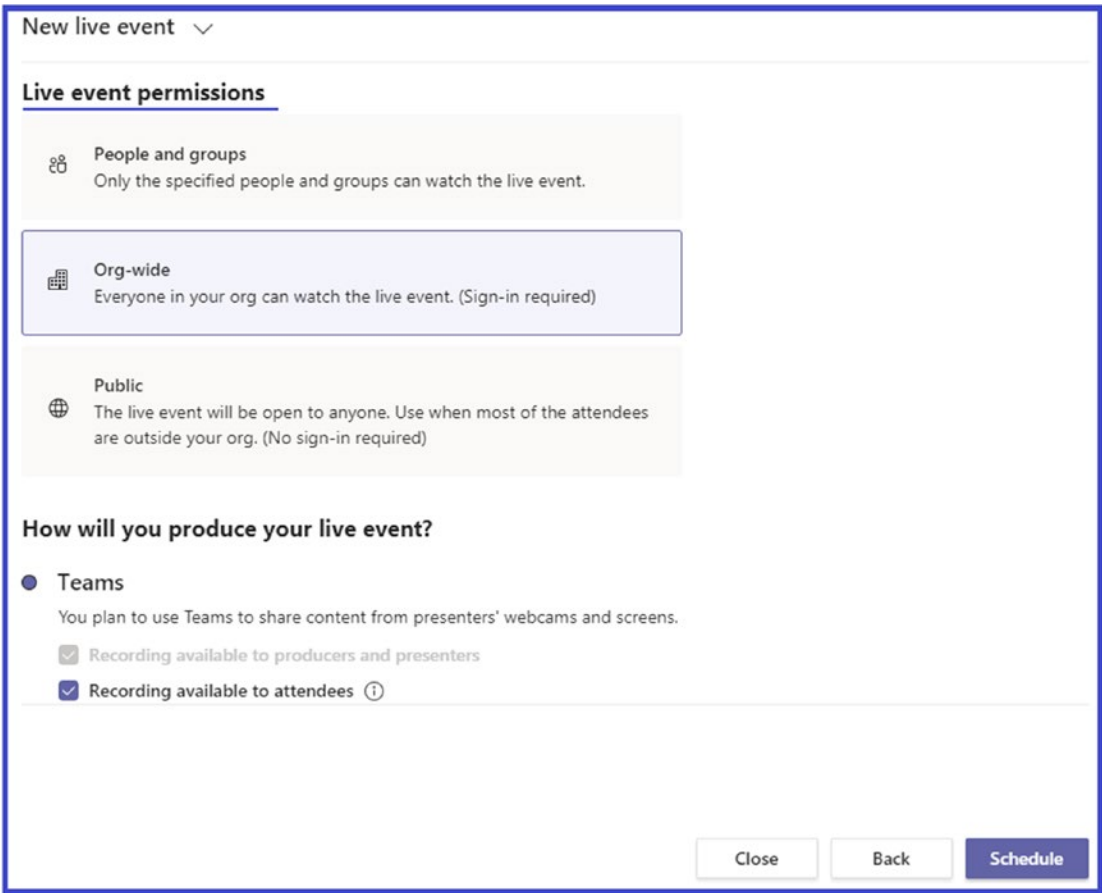


Figure 1-15. Scheduling a live event [67]

The next step is to set the production type by selecting a Quick start or third-party production, and then click Schedule to get the event scheduled. The examples in this book use the Teams meeting as a production type, as shown in Figure 1-16.

New live event ▼

How will you produce your live event?

Teams
 You plan to use Teams to share content from presenters' webcams and screens.

- Recording available to producers and presenters
- Recording available to attendees ⓘ
- Captions (preview)
- Attendee engagement report
- Q&A

An external app or device
 You plan to use another tool to share content. [Learn more](#)

Support
 Give attendees access to support info for your organization.

URL

Figure 1-16. Live event production type [67]

After the live event is scheduled, the event team can join the event. Figure 1-17 shows the producer view. At the top, you can see two windows, Queue and Live event. On the left you can always queue contents to follow, like presenting a slide after a video. Once the presentation is ready to begin, click Send Live so everyone can see it.

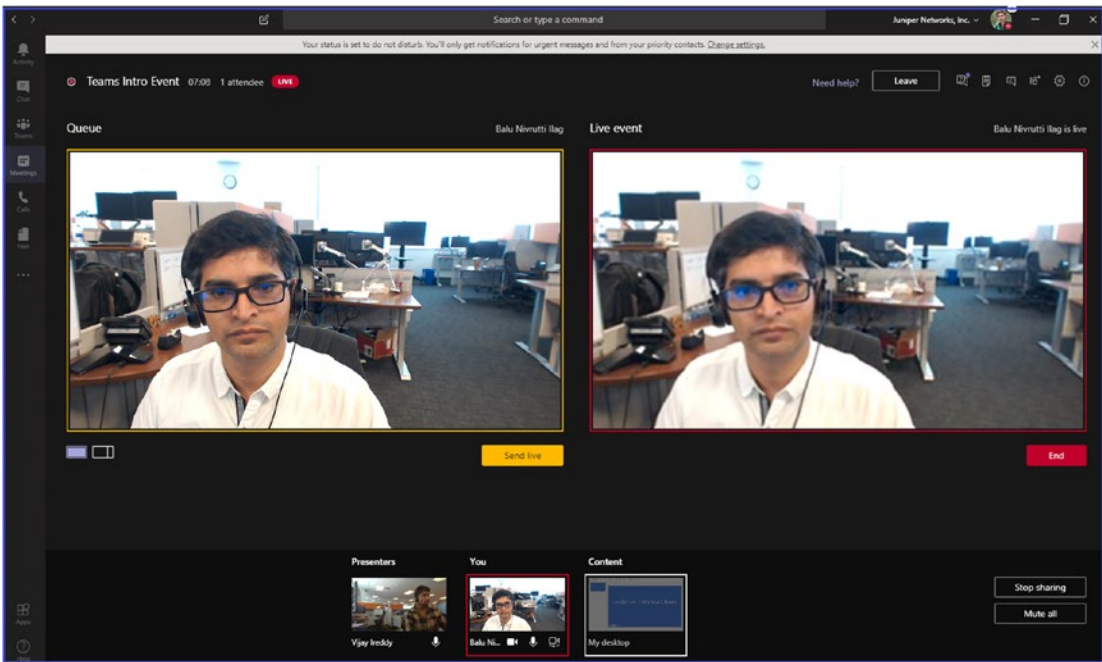


Figure 1-17. Live event producer view [67]

Attendees see whatever is presented under the Live event. At the bottom, audience members see different presenters. Event members can choose a different video, people, and content there.

If the presenter decides to schedule a meeting with the Q&A Manager to allow users to ask questions, then they can open or hide the Q&A Manager or keep it open all the time. The producer can send broadcast messages or share links during the session.

Teams Voice and Video Call and Meetings

Teams Voice and Video Calls

Microsoft Teams provides voice and video call capabilities with desktop sharing so that users can elevate their chat conversation to voice and video calls. Teams allows users to have a private, one-to-one call or group calls. This voice and video calling happens through VoIP. Teams voice and video calling has some network requirements, which are covered in Chapter 3 as part of organization preparation and readiness.

Users can make calls to their colleague as internal users, as well as external users, including guests, federated, and external phone calls. All of the following user types can leverage voice and video call capabilities.

- *Teams call with internal users:* These include corporate users who have an account in the same tenant; for example, balu@bloguc.com.
- *Call with guest users:* Guest users are invited to join one or two teams in your organization. That's why they are called guest users. Users who have a guest account in the same tenant can utilize calls and chat in Teams.
- *Call with federated (external) users:* Federated users are users of a different organization with federation configured between both organizations, where both organizations are using Teams; for example, bloguc.com and microsoft.com.
- *Phone (PSTN) call (audio only):* Teams allows users to make phone calls (voice only) using PSTN. However, the user must have enabled enterprise voice to make a phone call.

Microsoft Teams Meetings

Meetings provide a rich set of capabilities using various devices. Teams meetings provide a premeeting, during the meeting, and postmeeting opportunity to collaborate with members.

Microsoft Teams provides a better meeting experience by allowing users to organize easily, prepare, and follow up using pre- and postmeeting experiences like collaboration before the meeting using chat and meet-now. Users can be more engaged and productive by sharing content from desktop (Mac and Windows) or mobile devices and add video to meetings for face-to-face video. Finally, Teams meetings offer excellent audio and video quality and reliability from desktop (Windows and Mac) and mobile devices, phones, or conference rooms. The meeting organizer can also invite external users to join via a web browser. All this meeting experience builds on the foundation of the next-generation Skype infrastructure, and Office 365 services including Exchange, SharePoint, Stream, Microsoft AI, and Cortana [32].

For example, when a user schedules a Teams meeting to discuss project work, they will have the opportunity to engage in premeeting collaboration. For example, before the meeting, they can use the chat that is automatically created for that meeting to discuss the agenda and share files. Members of the team can join from all kinds of different devices, such as desktops (Windows or Mac), Android phones, and iOS phones. Office users can join from a Surface hub, if available. They can also share links, audio, video, and desktops so that everyone can see project materials. Also, they can record meetings so that users who were not able to join live can review the recording as well as any notes created during the meeting and continue collaborating in chat.

Teams meetings have some network requirements, and the network has a high impact on user experience, so it is essential to get the network right to have the best experience possible. Network assessment and bandwidth planning details are covered in Chapter 3.

There are different types of meetings that you can create in Microsoft Teams, depending on the nature of the meeting.

- *Private meeting*: When the user wants to have a meeting with individual people, but does not want the meeting to be visible to others.
- *Channel meeting*: When channel meetings are scheduled in the Teams team, all team members are automatically invited, and they will have access to the discussion and meeting recording if that meeting is recorded.
- *Ad-hoc meeting (Meet now)*: When the user wants to meet immediately without previously scheduling a meeting.

Teams meetings do have a meeting life cycle that includes after the experience before, during, and after the meeting.

- *Premeeting*: Users can have contextual conversations in Teams and prepare and discuss content before the scheduled Teams meeting.
- *During meeting*: Users can use face-to-face video, follow the action, share content, record the meeting with transcription, and join from a Teams room quickly.
- *Postmeeting*: Users can play back meetings with transcription, and they can share notes and engage in postmeeting chat and collaboration.

Who Can Attend the Teams Meeting?

As mentioned earlier, Teams allows internal (within the organization) and external (outside organization) participants, but there are more than just these two attendee types, and Teams allows all of them to join a Teams meeting. Depending on what type of attendee they are, however, they will have different information and options in the meeting.

- *Internal users:* These are corporate users who have an account in the same tenant; for example, balu@bloguc.com.
- *Guest users:* These users are invited to join one or two teams in your organization; that's why they are called guest users. Users who have a guest account in the same tenant can join the Teams meeting.
- *Federated users:* Federated users are users of a different organization with federation configured between both organizations. Both organizations are using Teams; for example, bloguc.com and microsoft.com.
- *Anonymous users:* Anonymous users have no account at all or an account in a tenant without a federation.

Remember that attendee type is determined at the meeting join time, and the user cannot change attendee type. For example, if a federated user forgot to sign in, that user will be treated as an anonymous user when he or she joins a meeting. If To join the meeting as a federated user, that user must leave the meeting and rejoin as federated by signing in.

Note It is not possible to promote users from one attendee type to a different attendee type. However, it is possible to demote or promote attendees as presenters or attendees in a Teams meeting.

Teams meetings, including Audio Conferencing details, are covered in Chapter 4. External access (federation) and guest access details are covered in Chapter 5.

Teams Phone System Overview

Microsoft Teams provides cloud voice facilities that are provided from Office 365 cloud services; additionally, it provides Private Branch Exchange (PBX) functionality and options for connecting Teams infrastructure to PSTN. The Phone System is the terminology that Microsoft uses for call control and PBX functionality.

What Does the Phone System Require?

Phone System provides call control and PBX Phone System capabilities that allow an organization to connect the Teams infrastructure to a PSTN provider that allows Teams users to make phone calls to external PSTN numbers. PSTN is essential because it is reliable, universal, and most important, it is deeply integrated with human life. Wherever users go, a phone is there, even when they are in an elevator or in the field somewhere.

Using Phone System in Teams allows users to place and receive phone calls, transfer calls, and mute or unmute phone calls. Calling functionality in Teams supports required Phone System features, such as call answering and initiating (by name and number) with an integrated dial pad, call holding and retrieving, call forwarding and simultaneous ringing, call history, voicemail, and emergency calls. Users can also use a different range of devices to establish calls, including mobile devices, headsets connected to a computer, and IP phones [71].

Now you understand why calling and Phone System is required in Teams. However, you should learn about the different components involved in Teams calling and Phone System that combine to provide complete Teams Phone System capabilities.

- *Phone System:* Teams Phone System is an add-on license on top of the Teams license that provides phone calling capabilities in Microsoft Teams. It turns on everything from simultaneous ringing to call queues to emergency calls.
- *Calling Plans:* These provide a way to connect Teams Phone System to the PSTN using Microsoft as a service provider through a Calling Plans license.
- *Direct Routing:* If an organization wants to continue with its existing PSTN service provider and wants to connect that on-premises session border controller (SBC) to the Teams Phone System, that can be

achieved Phone System through Teams Direct Routing functionality. It is another way to connect to the PSTN, where customers interface existing PSTN services to Teams through an on-premises SBC.

- *PSTN*: The PSTN is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication [70]. The PSTN needs to integrate Teams modern software with modern coding technique.

Teams Phone System details, including phone number management, Direct Routing, phone number porting, and call queues are covered in Chapter 4.

Microsoft Teams Licensing Requirement Overview

Microsoft has designed Teams licensing to provide maximum flexibility for the organization. After using basic Teams features including chat, internal calls, and content sharing, you as an admin can buy add-on licenses for more features, such as Audio Conferencing, Phone System, Calling Plans, and Microsoft Teams rooms.

Table 1-1 shows all Office 365 subscriptions that include Microsoft Teams.

Table 1-1. *Teams License*

Small Business Plans	Enterprise Plans	Education Plans	Developer Plans
Office 365 Business Essentials	Office 365 Enterprise E1	Office 365 Education	Office 365 Developer
Office 365 Business Premium	Office 365 Enterprise E3	Office 365 Education Plus	
Microsoft 365 for Business	Office 365 Enterprise E4 (retired)	Office 365 Education E3 (retired)	
	Office 365 Enterprise E5	Office 365 Education E5	
	Office 365 Enterprise F1		

Note All supported subscription plans are eligible for access to the Teams web client, desktop clients, and mobile apps.

- Is Teams meeting included in all Office 365 subscriptions?
 - No, Teams meetings are included in almost all the Teams licenses, with the exception of the F1 license, which doesn't have Teams meetings.
- What Teams license do I need to use for Teams Audio Conferencing?
 - If you want to use Teams Audio Conferencing, which gives you the ability to dial in and dial out from and to phones, this requires an additional license. An Audio Conferencing license is included in an E5 license or is available as an add-on for E1 and E3 licenses.
- Do I need a separate license to use the Teams Phone System and calling?
 - Yes, you need an add-on Phone System license or E5 license that includes a Phone System license on top of that. To use phone calling you need Calling Plans. Each user will need Phone System plus a domestic or domestic and international calling plan to allow them to make and receive phone calls.
- Is a Microsoft Stream license included in all Office 365 subscriptions?
 - A Microsoft Stream license, which provides the ability to record Teams meetings, requires E1, E2, E3, A1, A3, A5, Microsoft 365 Business, Business Premium, or Business Essential. Remember this is the case for both the organizer and the user who initiates the recording.
- Do I need any license to schedule a live event?
 - Yes, to schedule Live event, you need the following licenses:
 - An Exchange Online mailbox.

- An Office 365 Enterprise E1, E3, or E5 license or an Office 365 A3 or A5 license.
- A Microsoft Teams license.
- A Microsoft Stream license.

By default, Teams is turned on for all organizations. Administrators can assign user licenses to control individual access to Teams and allow or block which content sources are used.

Teams Integration with a Third-Party Application

Microsoft Teams provides greater customization within the Teams client by changing color themes and notifications within Teams customization for channel tab, connector, bot, and Microsoft apps, as well third-party apps integration. All this communication, collaboration, and customization happens securely with compliance capabilities.

Microsoft Teams provides a default set of apps published by Microsoft and by third parties that are designed to connect users, support productivity, and integrate commonly used business services into Teams. For example, users can use the Planner app to build and manage team tasks in Teams. These apps are available to organizations through the Teams Store. By default, all apps, including custom apps that your organization has submitted through the Teams Store approval process, are turned on for all users. Although all Microsoft apps and all custom apps are available by default, you can turn the availability of individual apps on or off. For efficiency, an organization-wide setting is available that allows you to turn all custom apps on or off for your entire organization.

Teams apps are a way to collect one or more capabilities into an app package that can be installed, upgraded, and uninstalled. The capabilities include the following:

- Bots.
- Messaging extensions.
- Tabs.
- Connectors.

Apps let you find content from your favorite services and share it right in Teams. They help you do things such as pin services at the top of a channel, chat with bots, or share and assign tasks. Microsoft recommends that you add featured apps such as Planner in your initial Teams rollout. Add other apps, bots, and connectors as you drive Teams adoption.

Managing apps policy and administration is covered in Chapter 5.

Summary

In this chapter, you were introduced to Microsoft Teams, its architecture, and the different components involved. You also learned about Teams service dependency, live events and Stream architecture, Phone System, licensing requirements, and Teams apps integration opportunities.

Now that you have completed this chapter, you should understand the following:

- Microsoft Teams architecture and different components.
- How Microsoft Teams interacts with SharePoint Online and OneDrive for Business.
- How Microsoft Teams interacts with Exchange.
- What live events are and their architecture.
- The uses of Microsoft Stream and its architecture.
- Teams Phone System and voice communication capabilities.
- Teams licensing requirements and add-on licenses.
- Microsoft Teams integration with Office 365 and third-party applications.

CHAPTER 2

Managing and Controlling Microsoft Teams

Microsoft Teams provides a variety of different policies for managing collaboration between users within teams and channels. You can control the general abilities of users to use chat, edit or delete their sent messages in conversations, and configure the collaboration features and settings that are available to them. You can also effectively manage the Microsoft Teams experience through different administrative tools.

In this chapter you will learn about the policies and settings to manage collaboration in teams. After this chapter, you will be able to do the following:

- Create and modify messaging policies.
- Design teams' policies for channel creation and discovery.
- Configure the organization-wide settings for teams.
- Manage the creation of private channels within the Teams client.
- Control the email integration of teams.
- Organize the file sharing functions from the Teams client.
- Understand how to set up channel moderation in teams.
- Understand Teams admin center details, including each and every task.

Microsoft Teams Authentication

How Microsoft Teams User Authentication Works

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. Azure AD is a cloud-based identity service, 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 user identity 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@bloguc.com, and I can sign in to Teams using my password.

Now you know Azure AD is a crucial part of the overall deployment and work of Teams. The million-dollar question is this: What is Azure AD, and how does Teams leverage it?

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 different licensing bundles including Small Business Plans like Office 365 Business, Enterprise Plans like Office 365 Enterprise E1, E3, and E5, Education Plans like Office 365 Education, and Developer Plans like Office 365 Developer.

Another important question occurs: How do I manage the cloud identity that is 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. [65]

Now, you know the importance of Azure AD, but how do you make sure the access permissions that users have as 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 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 is actually a method that allows Teams apps to understand that users have previously registered and logged in their credentials (like their work or institutional email and password) somewhere else, and they are not required to enter credentials again to initiate the Teams app.

Remember, Teams does have clients for Windows, macOS, iOS, and Android, so the user experience might be different for the different client platforms. 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 user account and password) and multifactor authentication (involving more than one factor, like verification over the phone or PIN along with user account and password). 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.

Using 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 multifactor authentication (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 to 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, there is another change. 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 if their desktop already requires MFA to sign in. If their desktop has previously required MFA to sign in, then users will automatically be signed in to 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 Modern Authentication, 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 Office 365 tenant, domain, or enterprise account itself. If there is a federation 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

1. First, the user enters a login credential in the Teams client.
2. The Teams client resolves DNS record ► `teams.microsoft.com`.
Once it resolves, the Teams client connects to Teams services.
 - A. Name: `s-0005.s-msedge.net` Addresses: `2620:1ec:42::132`
 - B. `52.113.194.132` - Aliases: `teams.microsoft.com` and `teams.office.com`

3. Teams services redirects the Teams client to Azure AD to get a token from Azure AD.
4. Azure AD gives the client access token to the Teams client.
5. The Teams Client gives the access token to Teams Cloud Service.
6. The Teams user is logged in to Teams services.

Manage and Configure Multifactor Authentication and Conditional Access for Teams

What Is Conditional Access in Authentication?

As you learned, Microsoft Teams leverages Azure AD for authentication and there are two different kinds of authentication: SFA MFA. However, an organization can consider securing the authentication by allowing Teams access through specific conditions like use of a specific operating system or version, client version, network subnets, 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.

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

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. Figure 2-1

shows signals on the right side; that is 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.

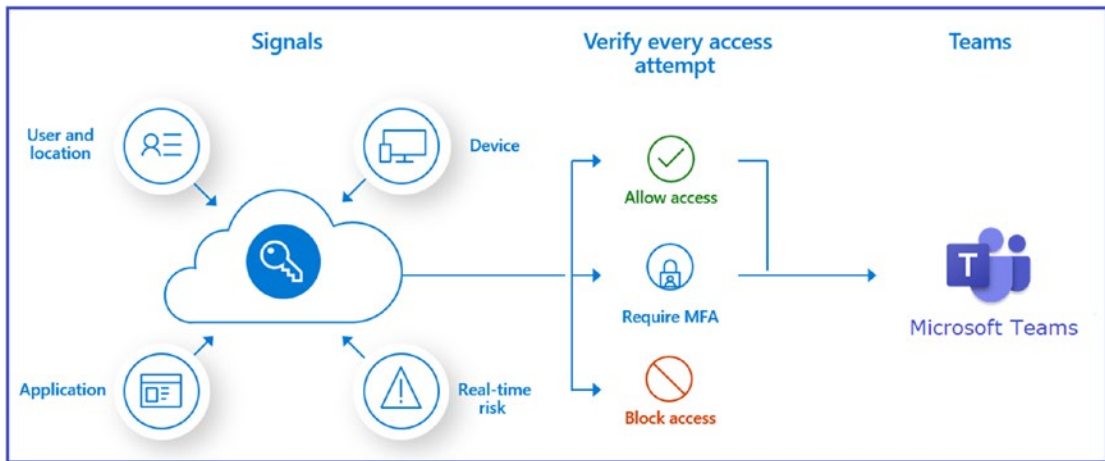


Figure 2-1. Azure AD conditional access [21b]

Managing Teams, Channels, and Their Types

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 2-2. Then select Join or Create a Team.

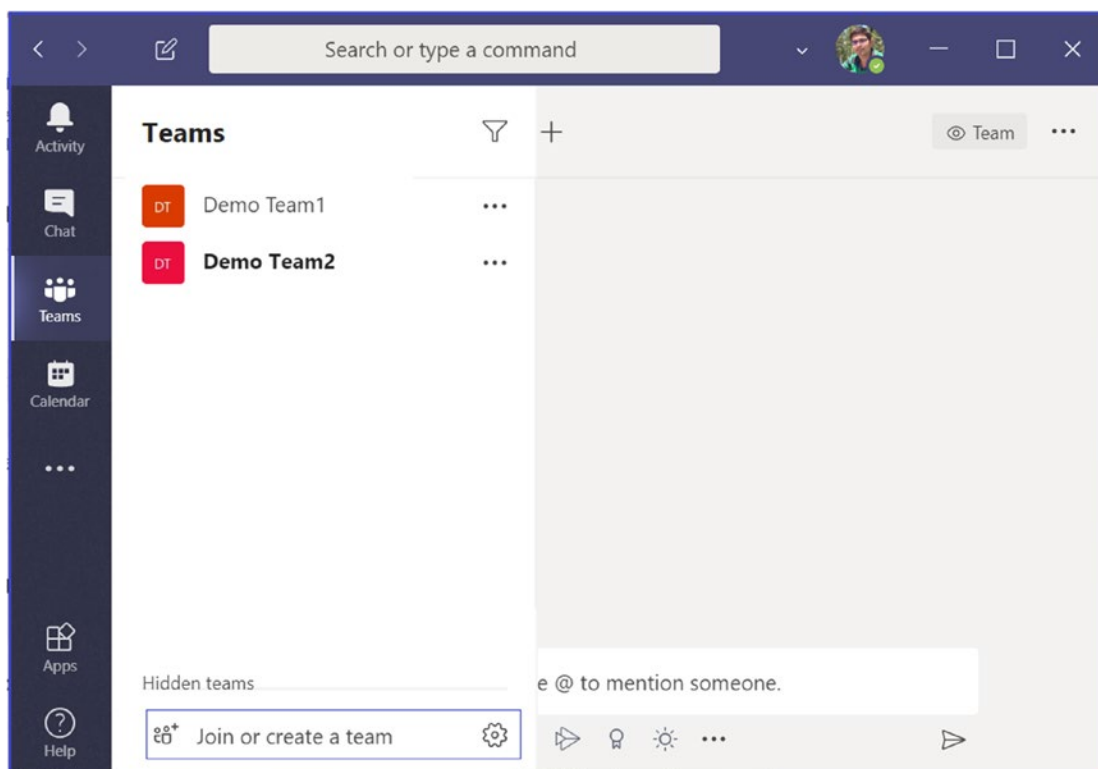


Figure 2-2. Create or join teams

2. Once the Join or Create Team page opens, click Create Team, as shown in Figure 2-3.

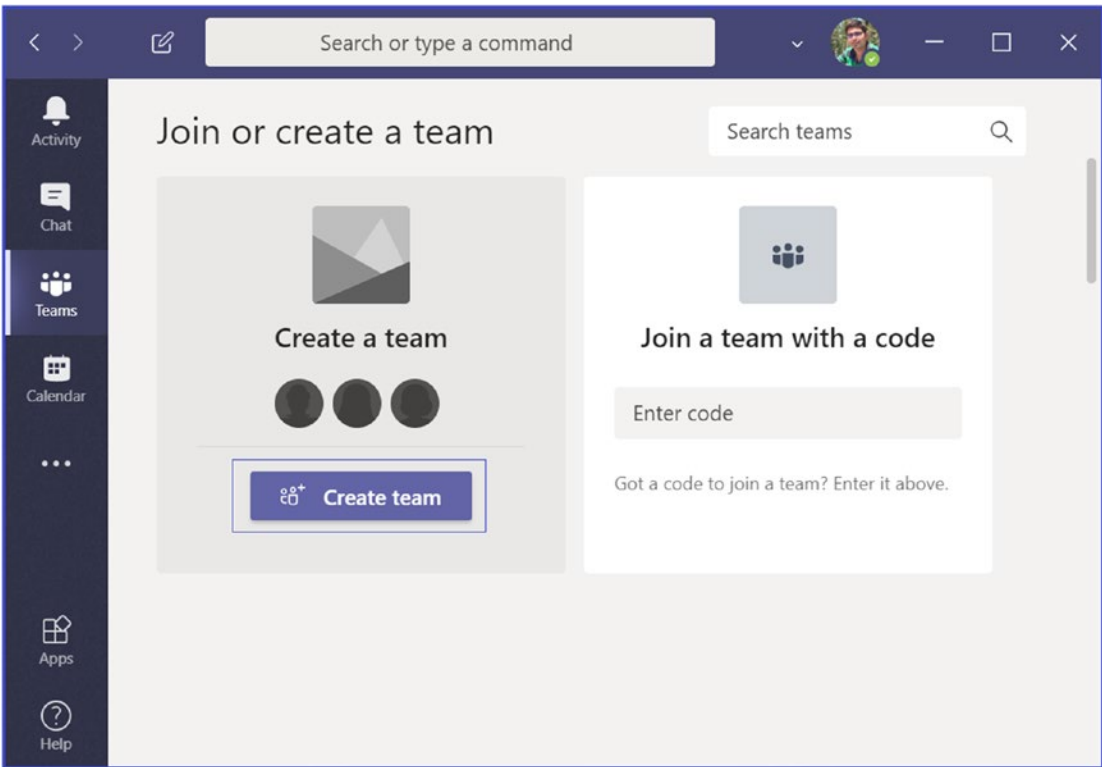


Figure 2-3. Create Team button

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 2-4 Build a Team from Scratch is selected.

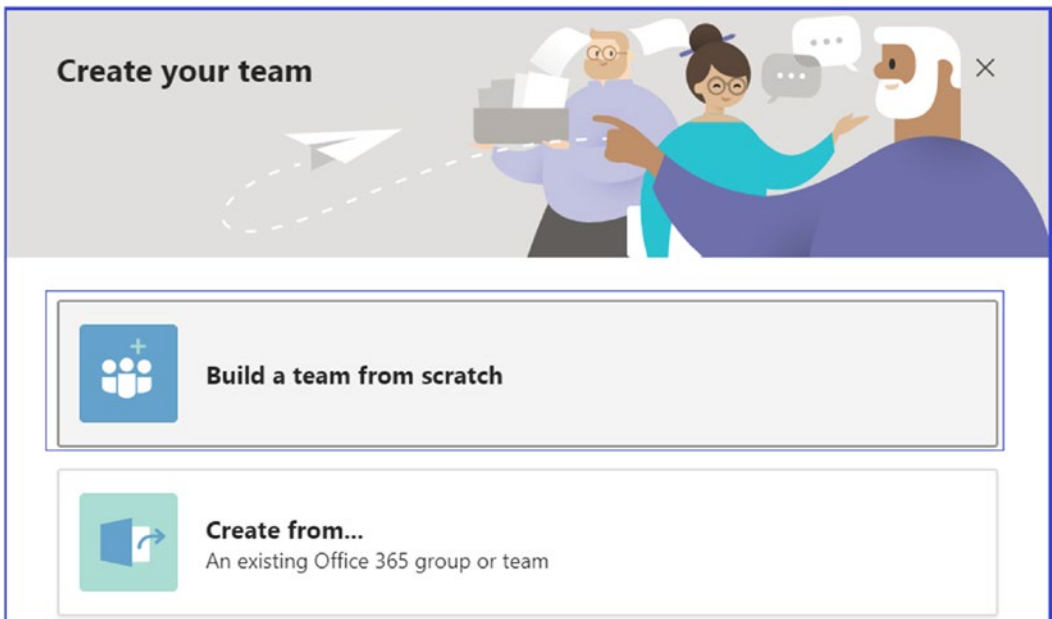


Figure 2-4. Select an option to create a team from scratch or use an existing Office 365 Group

4. After selecting Build a Team 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 2-5 shows selection of a private team.

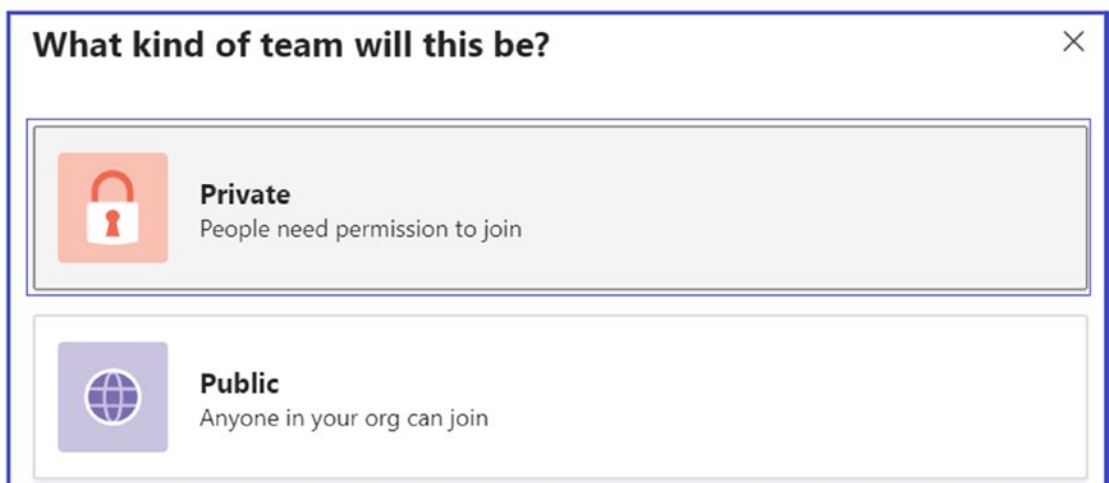


Figure 2-5. Team type can be private or public

- Next, provide an appropriate name and description for your team. Figure 2-6 shows the name Teams Administration 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.

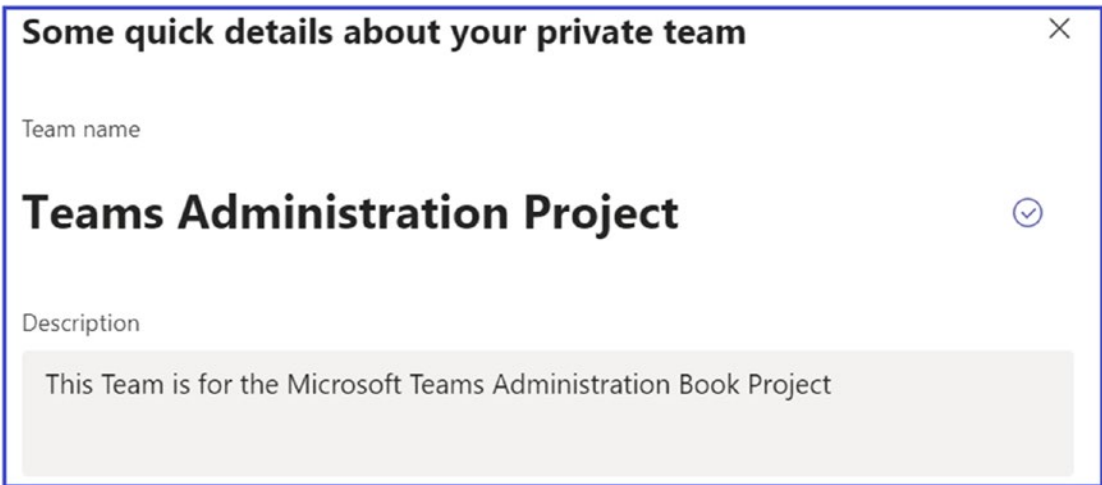


Figure 2-6. Team name and description

- Next, add members for your team after team creation. Once you add member, click Close to exit the member adding window. Figure 2-7 shows an added member Balu Ilag.

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

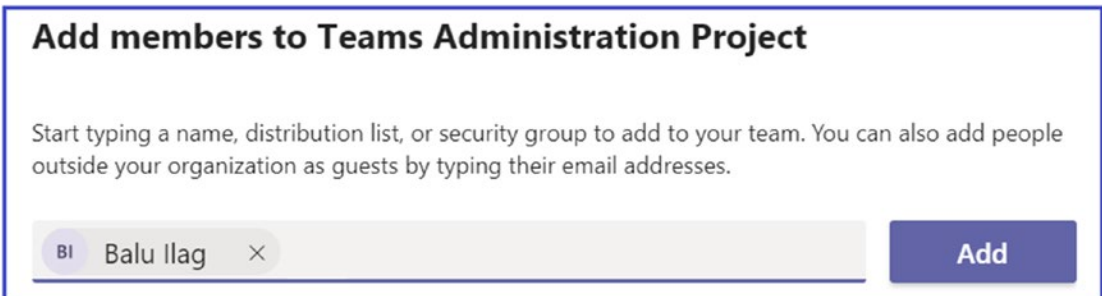


Figure 2-7. Add a team member

- Now you will see the team is created and a default channel is also added, General. Figure 2-8 shows a team named Teams Administration Project with the General.

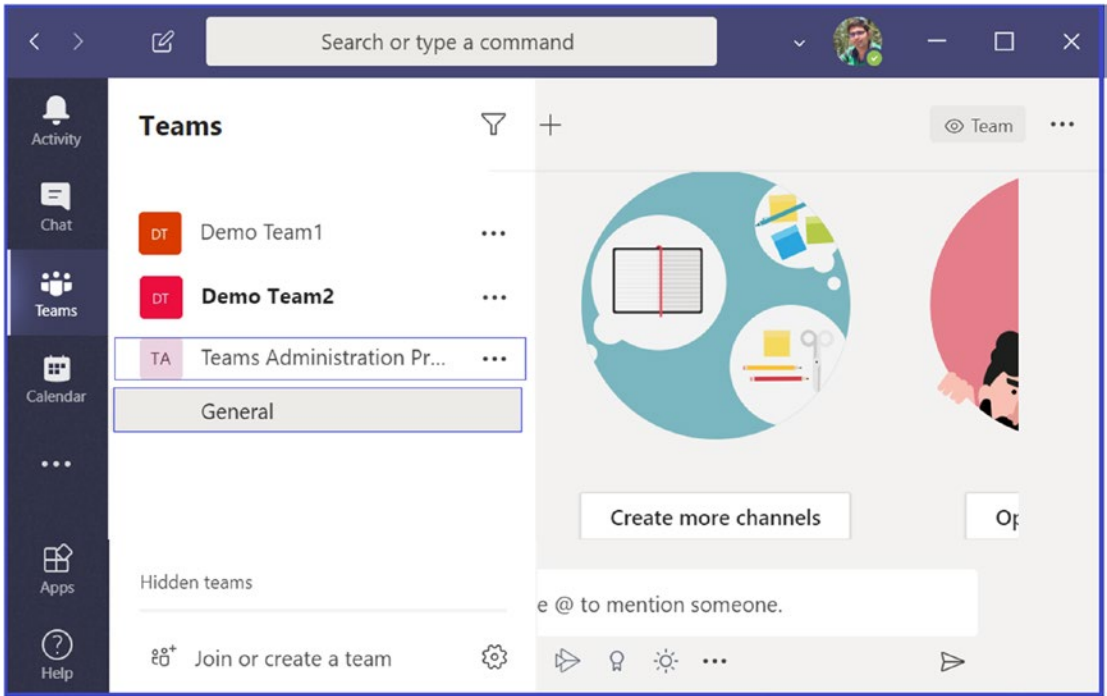


Figure 2-8. Team created with general channel

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

Creating a Channel in a Team

Creating channel is very easy.

- Click ... next to team name to display multiple options. From that list, select Add Channel to create a channel, as shown in Figure 2-9.

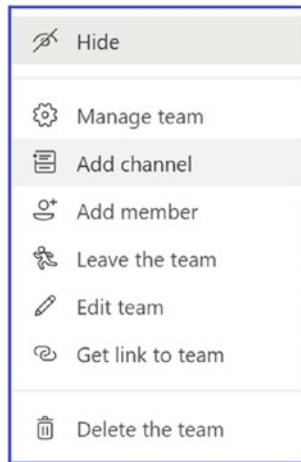


Figure 2-9. Adding a channel

2. After selecting the Add Channel option, 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 2-10 shows the Standard channel privacy type selected. Remember, there are two privacy modes.
 - *Standard:* This privacy mode allows anyone (team members) to access this channel content within the team.
 - *Private:* This privacy mode allows only a specific group of users to access this channel content. These users are added by the owner of the channel.

Create a channel for "Teams Administration Project" team

Channel name
Chapter1

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

Privacy
Standard - Accessible to everyone on the team

Automatically show this channel in everyone's channel list

Cancel Add

Figure 2-10. *Creating a channel and selecting a privacy mode*

Click Add to create the channel. Figure 2-11 shows the newly created channel and default features available to use. After channel creation, it will show posts and file Wiki tabs. You can add additional tabs by clicking the plus sign icon.

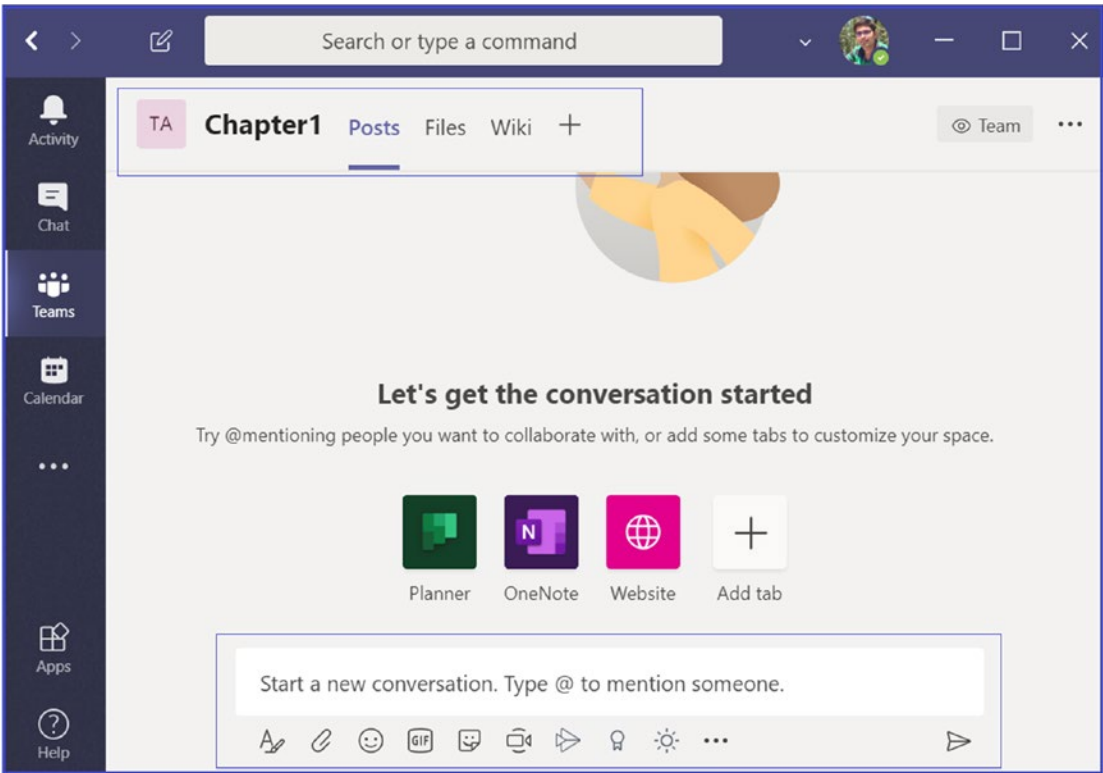


Figure 2-11. Channel created

When you click on the plus sign (+) icon that is marked Add Tab, you will see multiple applications that can be added as tabs to you channel, as shown in Figure 2-12.

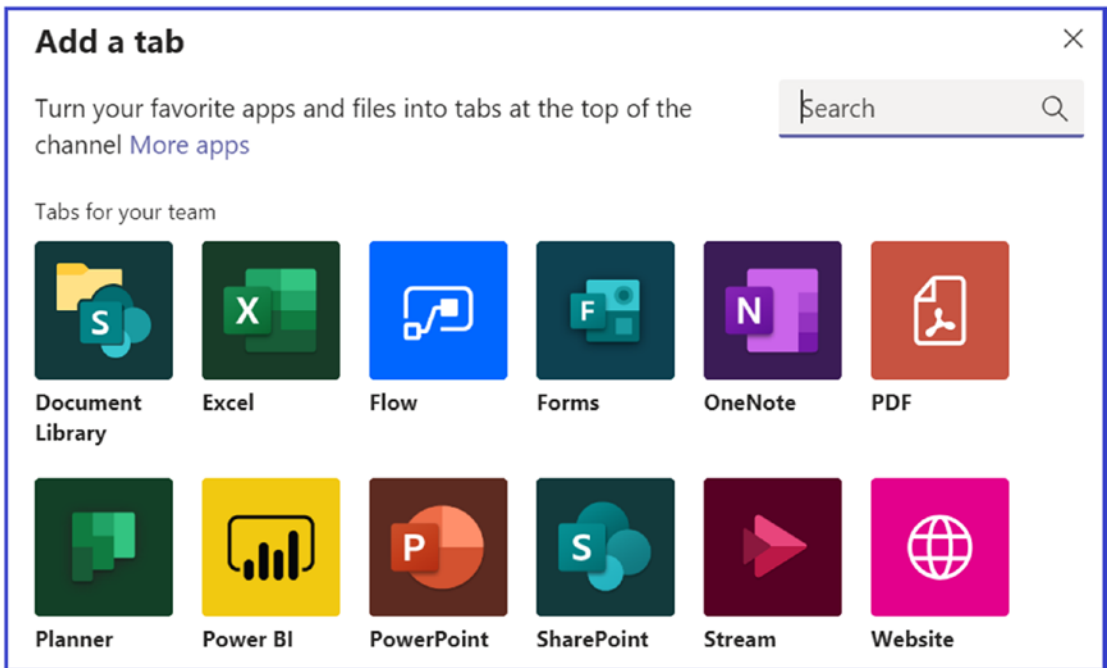


Figure 2-12. Applications to add as tabs

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 enabled file sharing. Microsoft is making sure that information shared in a private channel is only available to the private channel members, not for 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 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 the 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 a 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 ability at the tenant level or at the team level.

For the tenant level, you as an admin can define a policy in 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 2-13.

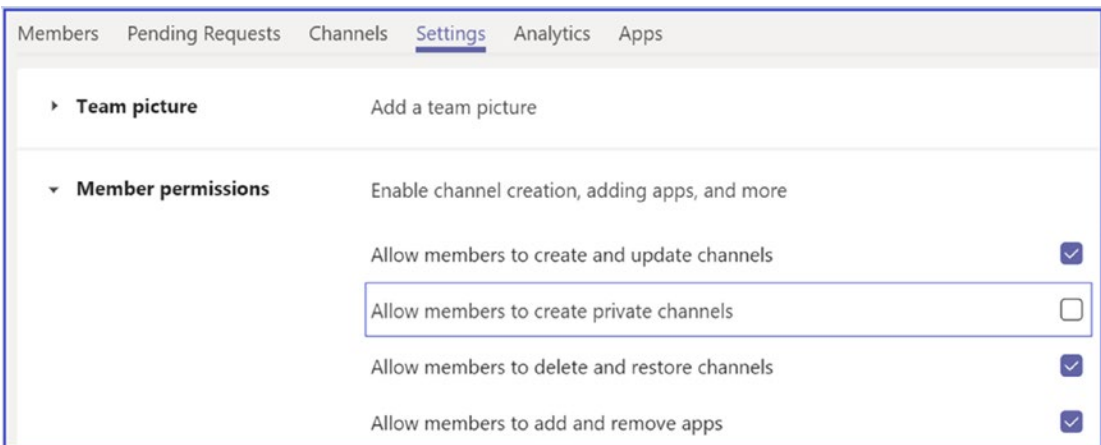


Figure 2-13. Private channel restriction setting

Creating a Private Channel

A private channel is accessible to specific people or a group who are added as 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 option 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 2-9. 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 2-14 [28a].

The screenshot shows a dialog box titled "Create a channel for 'Teams Administration Project' team". It contains three input fields: "Channel name" with the text "Acknowledgement", "Description (optional)" with the text "Help others find the right channel by providing a description", and "Privacy" with a dropdown menu showing "Private - Accessible only to a specific group of people within the team". At the bottom right, there are two buttons: "Cancel" and "Next".

Figure 2-14. 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 2-15.

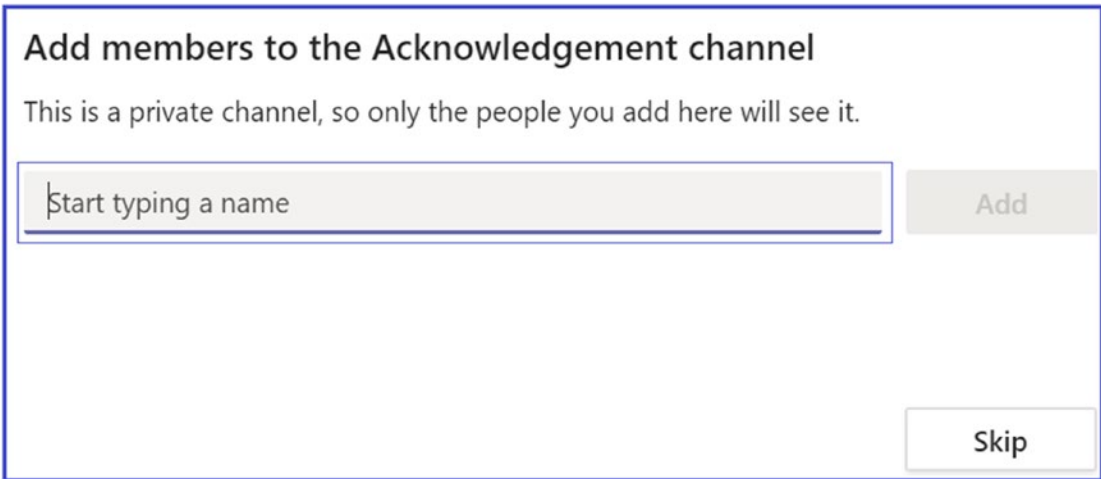


Figure 2-15. Adding members to a private channel

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 2-16 shows that the Acknowledgement channel is a private channel.

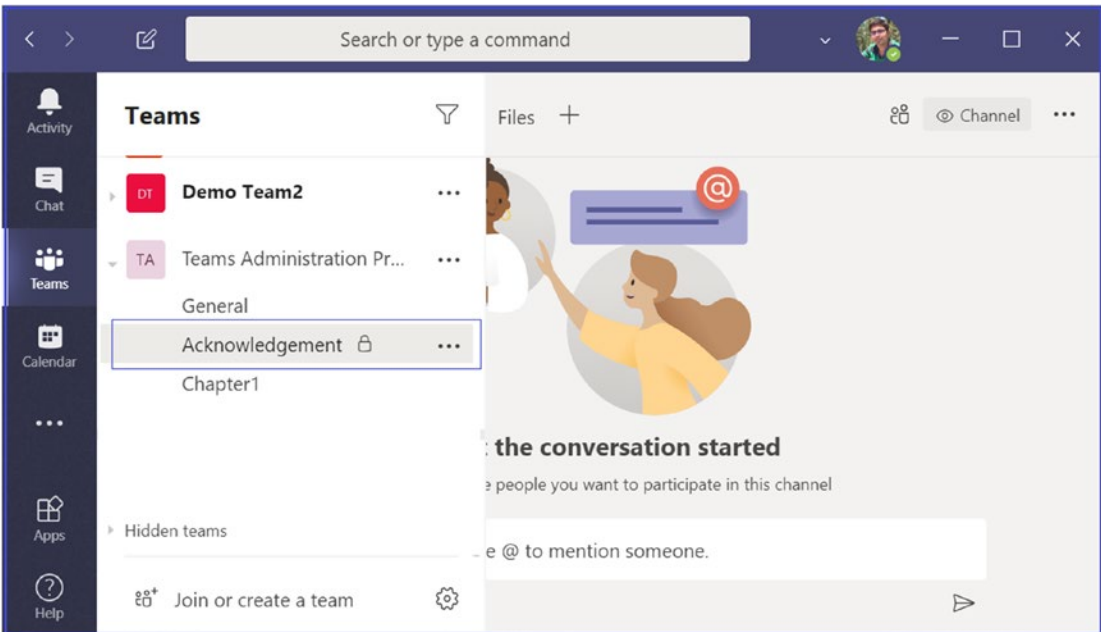


Figure 2-16. Private channel with a lock icon next to its name

Team Management Options

You as a team owner can manage your team settings. Figure 2-17 shows the team management settings that are available, including membership, guest access, and more.

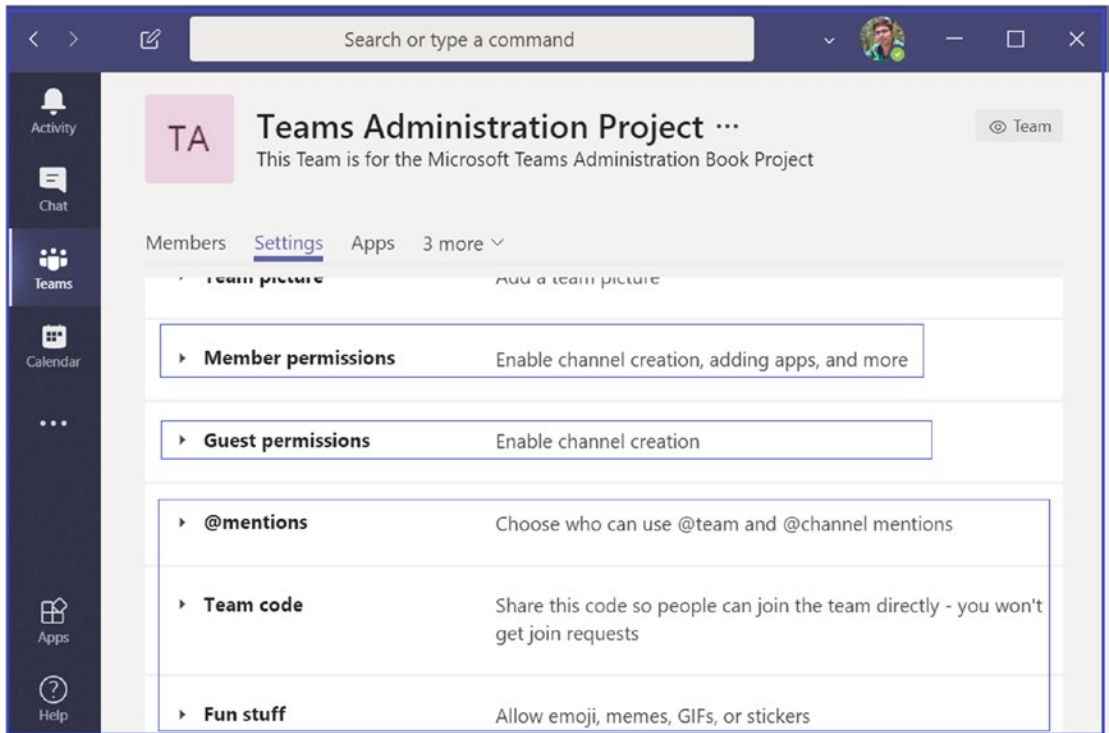


Figure 2-17. Team settings

Using the guest permissions settings, you can manage guest access for creating, updating, and deleting channels, as shown in Figure 2-18.

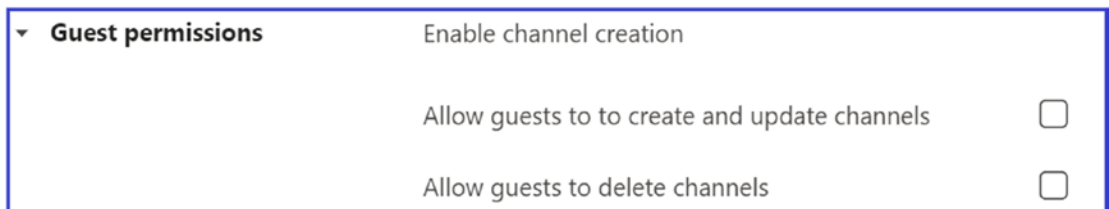


Figure 2-18. Guest permissions settings

The team owner can manage members permissions such as, who can create or add apps, update channels, create private channels, and so on. Figure 2-19 shows all available member permissions settings.

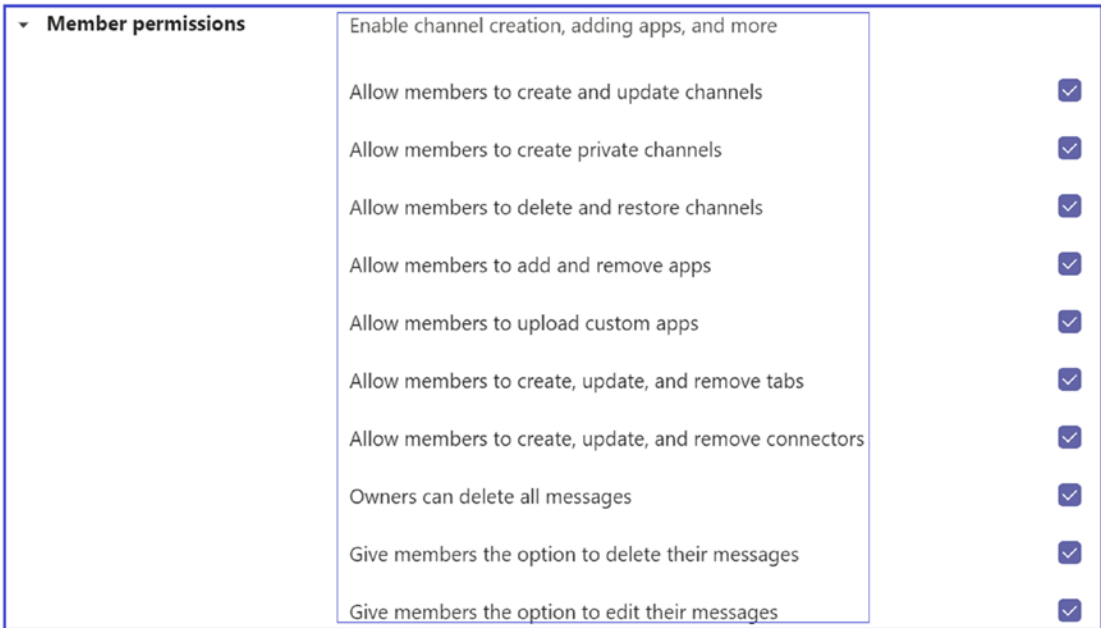


Figure 2-19. Member permissions to control member access

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, like 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 team owner, members, and guests have to execute tasks. The listed permissions are based on the Teams desktop client, so using the Teams mobile client you might see some differences.

Table 2-1. *Team Owner, Member, and Guest Permissions to Execute Tasks [19a]*

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 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. [76]

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 and (Windows 32- and 64-bit, macOS and Linux DEB/RPM 64-bit) and mobile (iOS and Android) clients, as shown in Figure 2-20.

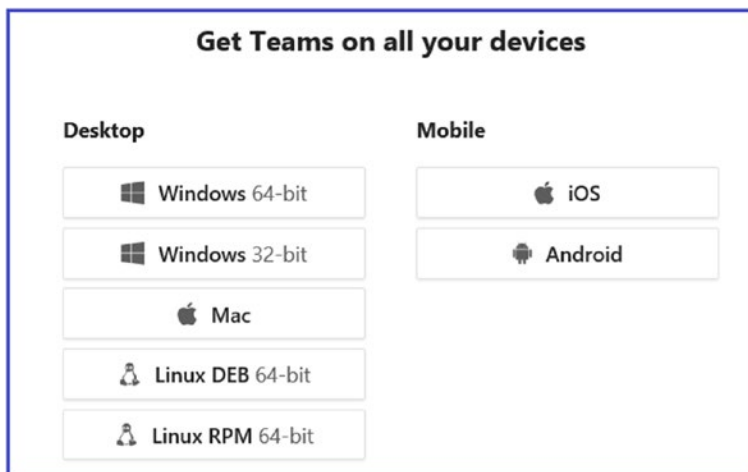


Figure 2-20. Get Teams client for all devices

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 Monthly channel and Semi-Annual channel. For more information you can visit the Microsoft documentation for deploying Teams at <https://docs.microsoft.com/en-us/DeployOffice/teams-install>.

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 [76a]*

Component	Requirement
Computer and processor	Minimum 1.6 GHz (or higher) (32-bit or 64-bit)
Memory	2.0 GB RAM
Hard disk	3.0 GB of available disk space
Display	1024 x 768 screen resolution
Graphics hardware	Minimum of 128 MB graphics memory
Operating system	Windows 10, Windows 8.1, Windows 8, or Windows 7 Service Pack 1 in 32-bit and 64-bit. For the best experience, use the latest version of any operating system.
.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	For better experience with video calls and online meetings, we recommend using a computer that has a 2.0 GHz processor and 4.0 GB RAM (or higher). The optional blur my background video effect requires a processor with Advanced Vector Extensions 2 (AVX2) support.

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 for 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 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 2-21 shows the Teams directory.

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

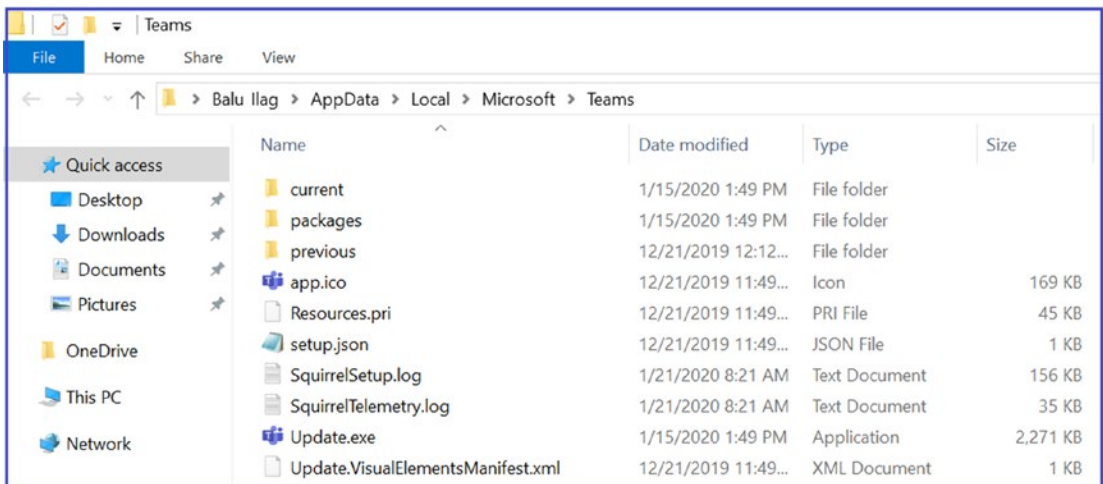


Figure 2-21. Teams installation directory

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

Microsoft Teams Desktop Client MSI Deployment

Microsoft allows for Teams (MSI) client rollout through existing standard deployment processes such as Group Policy, SCCM, Intune, or third-party tools. You as 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 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.

Teams MSI installer also allows you to disable client auto-start. 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, MSI installer allows you to disable the initial auto launch of Teams. Also, the Teams client shortcut will be placed on the user's desktop [76].

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

To disable the Teams client auto start 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 auto start.

Managing Teams Desktop Client

Microsoft made Teams client management simple and easy to operate.

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, then click Uninstall. After uninstallation, delete the Teams directory recursively under %LocalAppData%\Microsoft\Teams.

Microsoft has provided the cleanup script for uninstallation steps for SCCM, which you can find from <https://aka.ms/AA2jisb>.

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 in to 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 three versions, the Teams client cannot sign in before client updates.

Managing Teams Client Configuration

Currently 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 Teams admin center policies for all the clients. As another example, Outlook add-ins can be enabled or disabled through Teams admin center meeting policies. However, there is nothing that can be managed or controlled via Group Policy or registry key. Microsoft might or might not change this behavior in the future.

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 Outlook client (you can use Task Manager to completely close `teams.exe` and `outlook.exe`; see Figure 2-22).

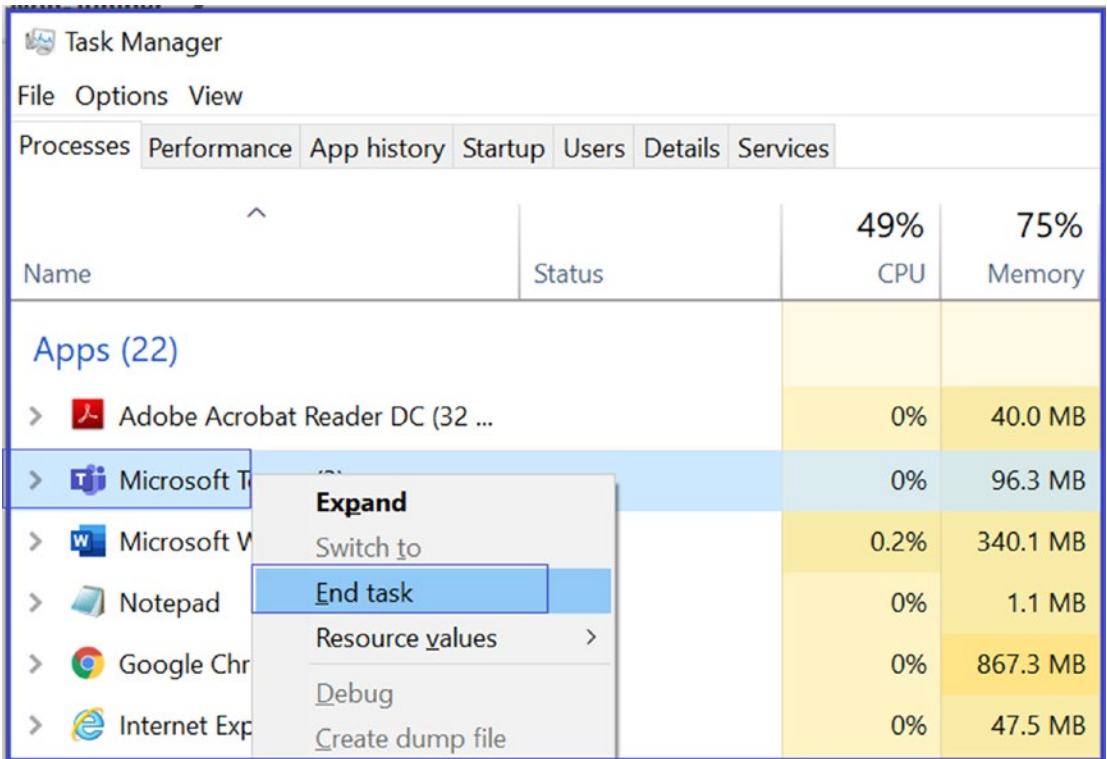


Figure 2-22. Close the Teams client completely

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 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 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 the same.

Virtual Desktop Infrastructure (VDI) is virtualization technology that hosts a desktop operating system and applications on a centralized server in a datacenter. With VDI, users can enjoy a fully personalized desktop experience with a fully secured and compliant centralized source [76a].

Deploying 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 [76].

Note Teams mobile app distribution is not currently supported using an 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 Teams desktop and mobile clients in your organization, the next important step is to monitor the Teams client usage per operating system or device. You can monitor the Teams client device usage using 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 then select Usage. On the Usage page, select Microsoft Teams and choose Device Usage. Figure 2-23

shows an example Teams client device report. On the report page, you can choose Users or Distribution; Figure 2-23 shows the Teams device distribution report.

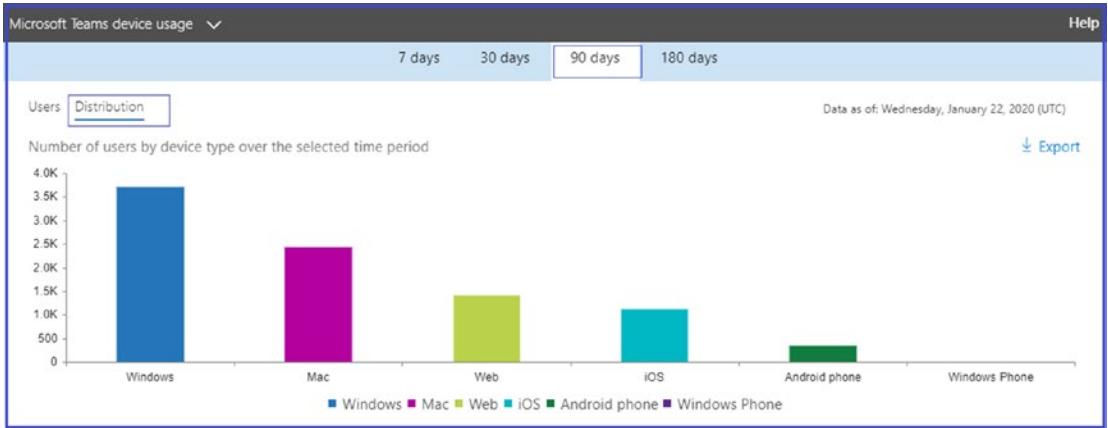


Figure 2-23. Teams client device usage report

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 event 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 topic, 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 using Microsoft Stream for meeting video recording and sharing content [38].

After learning this topic, you will be able to do the following:

- Configure live events settings.
- Manage and create live events 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 10,000. Live events scales online meetings to audiences with thousands of concurrent viewers. In the background, it leverages artificial intelligence for meeting assistance for features like captions and translation. Captions are very 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, like 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 datacenters, 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 a 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 an Office 365 Enterprise E1, E3, or E5 license or an Office 365 A3 or A5 license. User 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 Team 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 Teams admin center and using PowerShell.

Configuring Live Event Settings Using Teams Admin Center

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

1. Log in to Microsoft Teams admin center with your admin credential (you must have Teams service admin or global admin permission configure live event settings).
2. After you log in to Teams admin center, navigate to Meetings and then select Live Events Settings (see Figure 2-24). 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.

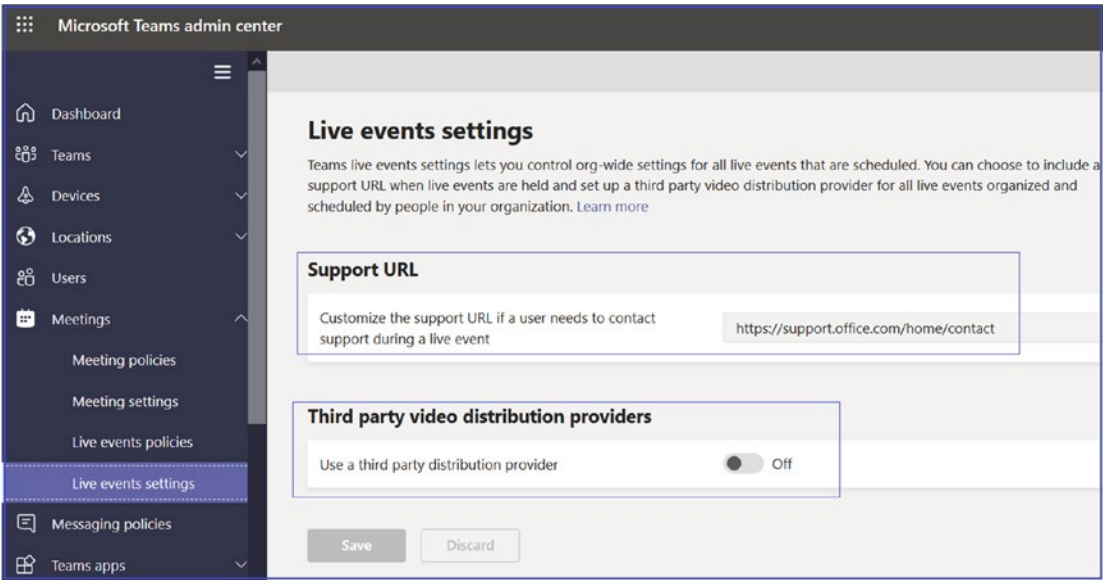


Figure 2-24. Live event settings

If you have a third-party distribution provider, select the appropriate one. The example shown in Figure 2-25 has Kollektive 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 two distribution providers, Hive and Kollektive, both of which work the same way.

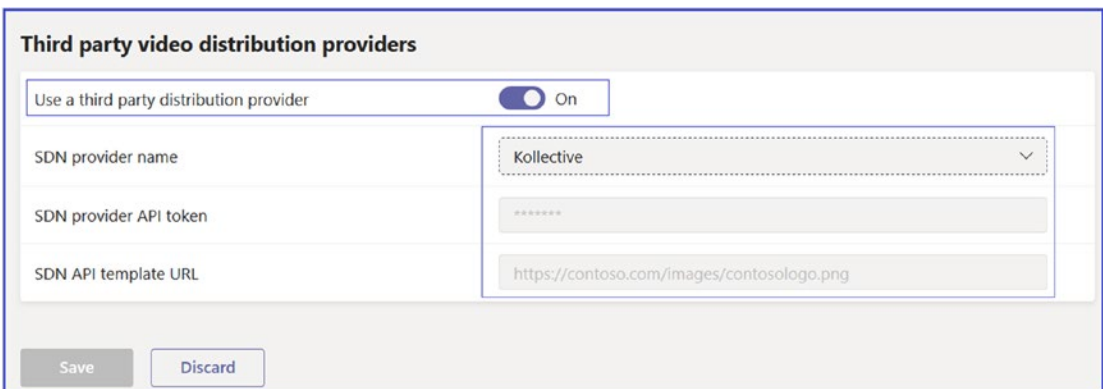


Figure 2-25. Third-party distribution providers

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

Configuring Live Event Settings Using PowerShell

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

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

For 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
-AllowSdnProviderForBroadcastMeeting $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 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, Global (Org-wide default) live events policy is available. Admins can modify this policy or create one or more custom live events policies. After a custom policy is created, it should be assigned to a user or groups of users within the organization.

Note 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 2-26 shows the default policy that will have settings including live event scheduling 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.

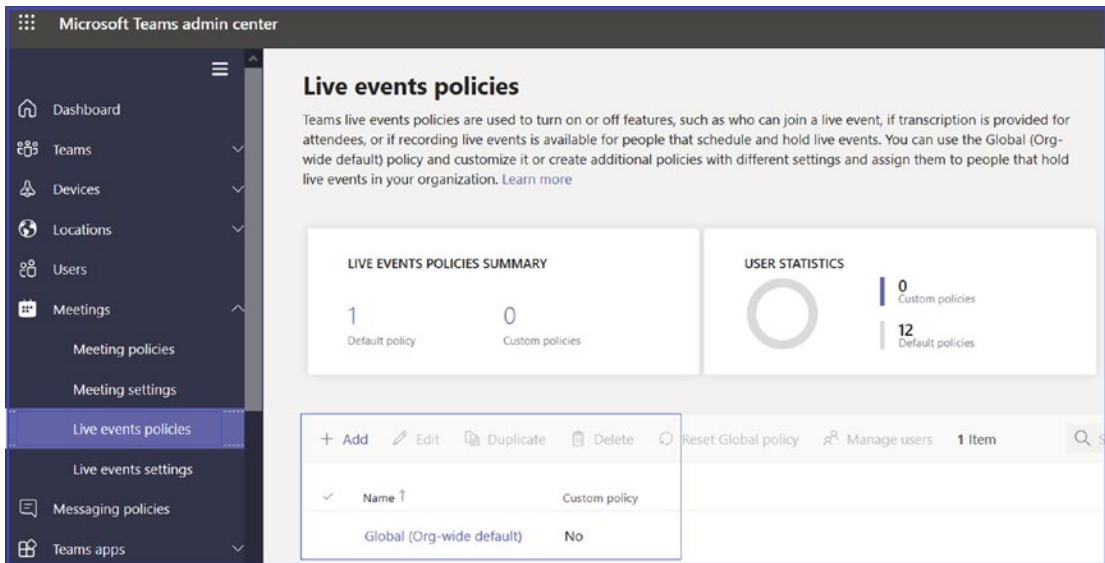


Figure 2-26. Default Global (Org-wide) policy in live event

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

Creating New Live Event Policy Using Teams Admin Center

Log in to 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 Teams admin center, navigate to Meetings, and click Live Event Policies. Select the + Add button, then enter the required inputs, as shown in Figure 2-27.

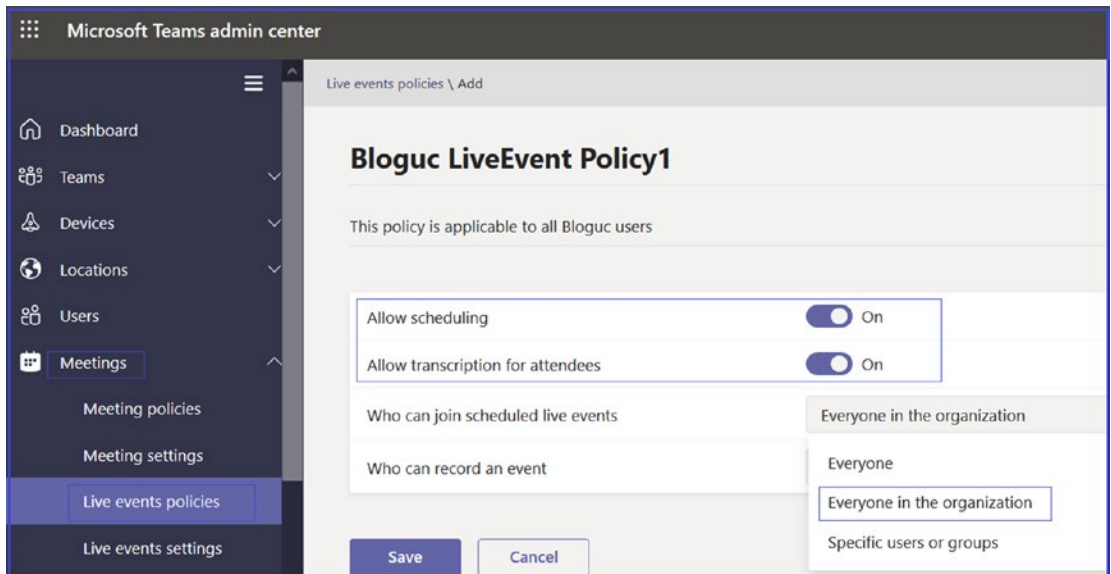


Figure 2-27. Create a new live event policy

On the new event page, type a meaningful name for your policy, and optionally type a description. This example uses the name Bloguc 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 2-28 shows Always Record as the selected setting.

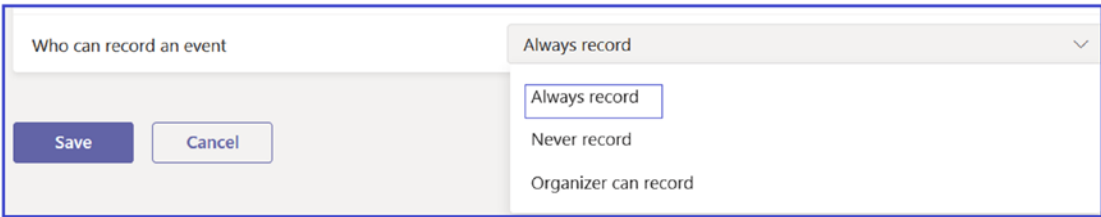


Figure 2-28. *Who can record a live event*

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.

1. You can access Microsoft Stream by visiting this URL: <https://web.microsoftstream.com>.
2. 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 you, Videos, Channels, People, and Groups settings are available for your organization, as shown in Figure 2-29.

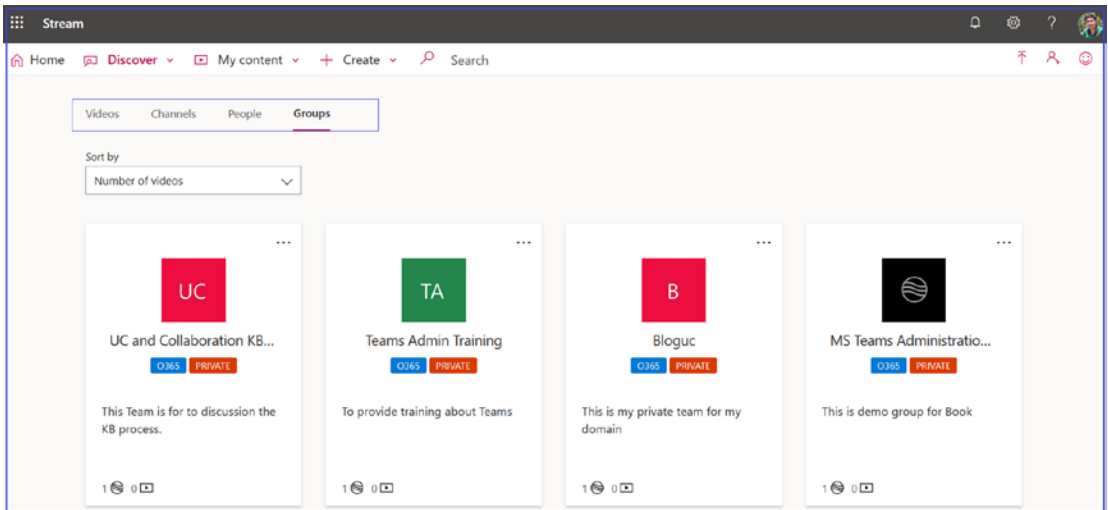


Figure 2-29. Microsoft Stream Groups view

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, Yammer, Planner, and so on, you can start using those groups in Stream right away [69a].

In Microsoft Stream, you can use channels and groups to organize and grant permission to your videos. Specifically, groups in Stream are used for controlling video access and organizing 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 like 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

Managing Teams Using Microsoft Teams Admin Center

Microsoft Teams admin center is one place where most of the Teams service-side configuration and management resides. Using 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 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 topic will provide extensive details about Microsoft Teams administration including all that Teams admin center provides.

Accessing Teams Admin Center

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

Apart from 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 as well. It's entirely up to you to use whichever solution is suitable for the Teams management perspective in your organization.

Understand 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.

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 Service Administrator*: 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.

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 Teams 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 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 only see the Users and Call Quality Dashboard options on the Teams admin center dashboard.

I have logged in to Teams admin center (<https://admin.teams.microsoft.com/>) using my Teams Service Admin role permission to see all admin tools and options to manage Teams for my demo tenant. Figure 2-30 shows the ideal Teams admin dashboard that a Teams admin can see.

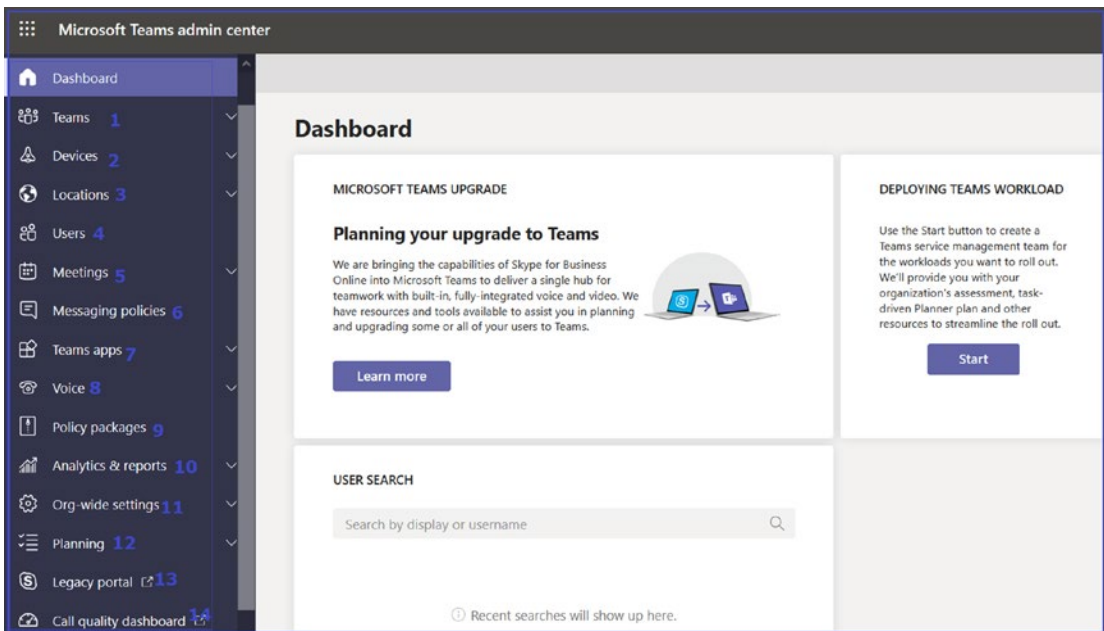


Figure 2-30. Teams admin center dashboard

Admin Center: Teams Tab

The first management tab shown in the Teams admin center is Teams. Using this tab you can manage your organization team and channels that users have created.

- a. *Manage Teams:* When you click Manage Teams, you will see a global view of teams that have been created in your organization. As an admin, you can manage each and every team from this tab. You can also add or create teams. For example, you can see four teams created in Figure 2-31.

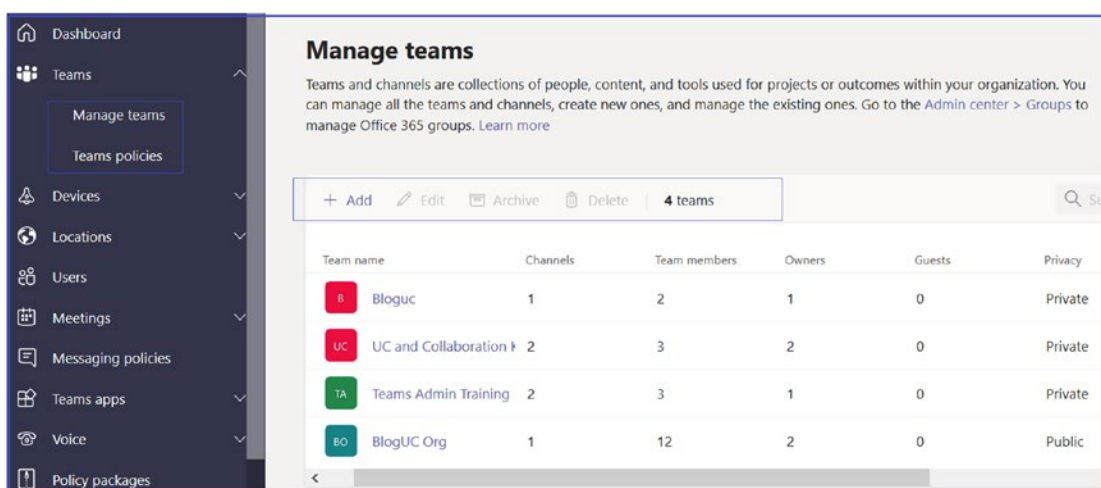


Figure 2-31. The Manage Teams tab

To manage an individual team, click the team name to open a management page for the team. You can add or remove members, modify channel, 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 2-32.

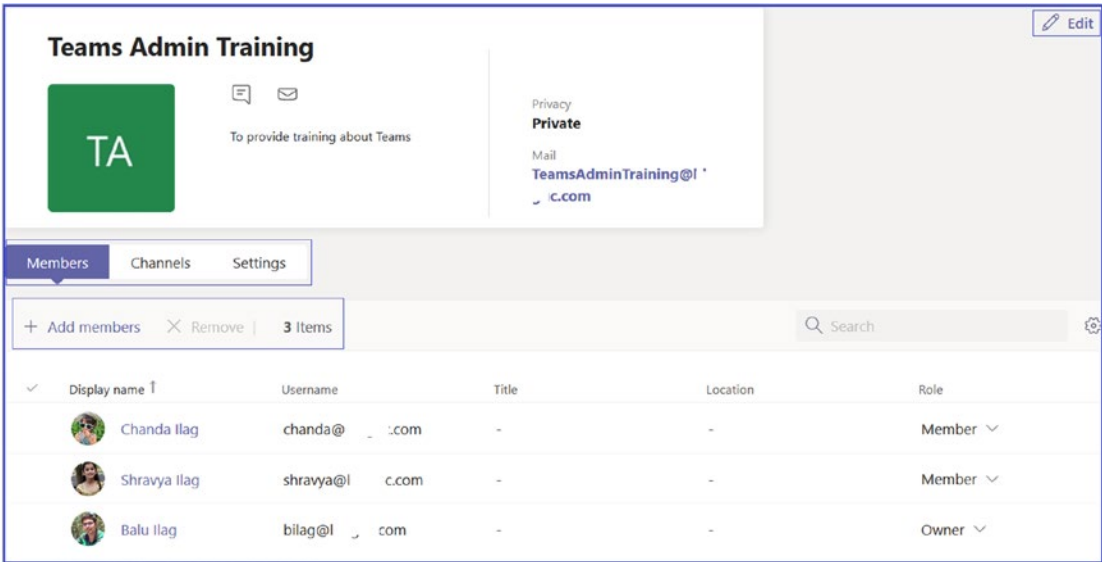


Figure 2-32. Manage a team and channel

Creating and Managing Teams Policies

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 that 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. Figure 2-33 shows the Teams policies tab.

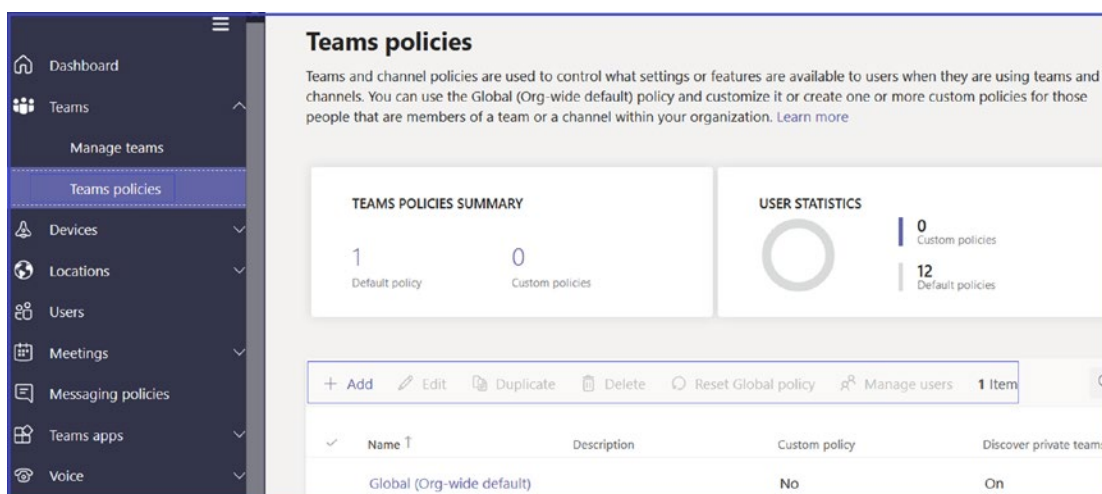


Figure 2-33. Teams policies

Creating a New Teams Policy

To create a Teams policy, log in to Teams admin center, then 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 discovery of private teams and creation of channels. Figure 2-34 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 Teams Global policy.

- *Discover Private Teams:* This setting lets people search for and find private teams that have been created. When they find the private team, they can then request access to it.
- *Create Private Channels:* You can create private channels for a specific group of users in your organization. Only those people who are added to the private channel will be able to see and write messages.

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.

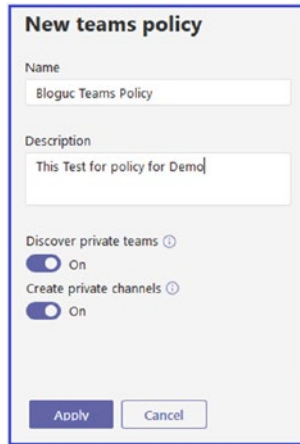


Figure 2-34. Creating a new Teams policy

Admin Center: Devices Tab

Managing and Deploying Teams Phone Endpoint

Microsoft Teams has clients available for 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.

Phones

Devices allows you to control the IP phones and peripheral devices such as headsets and webcams that have been certified for use with Teams. You can create and upload configuration profiles for each type of device you have, so you can make changes to their settings, including applying firmware updates so they can be easily updated.

You will see all phone devices under Phones ► All Devices and then you can create a configuration profile (see Figure 2-35).

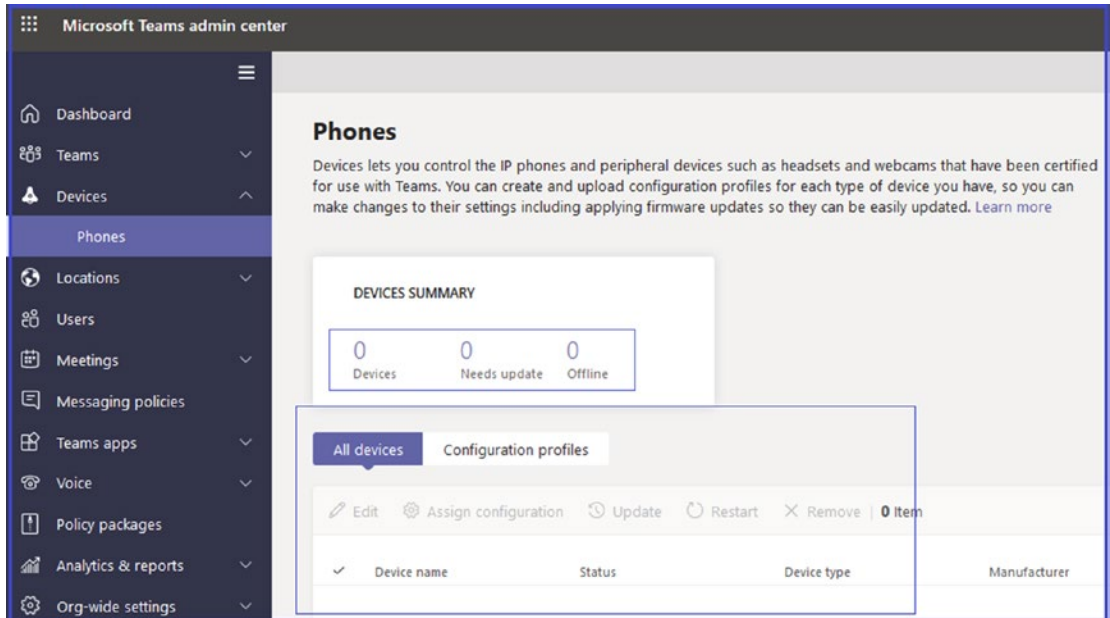


Figure 2-35. Phone devices in Teams admin center

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 Microsoft Teams admin center. On the left navigation pane, select 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. For example, Figure 2-36 shows a sample configuration.

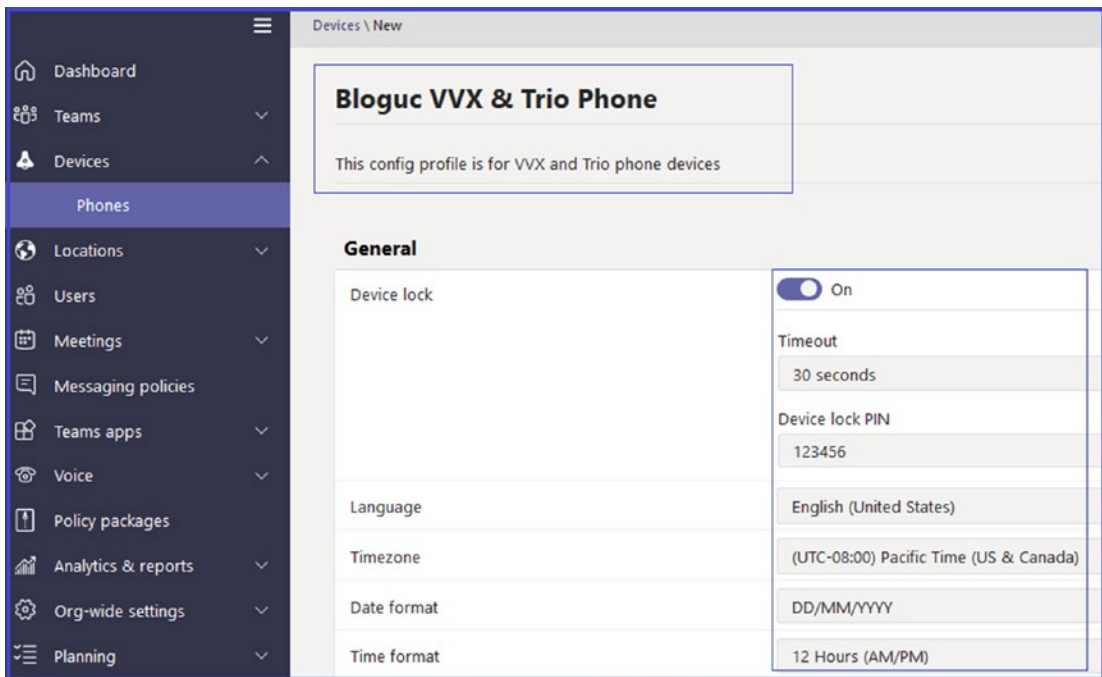


Figure 2-36. Phone configuration

- b. In the Device Settings section, select whether you will you enable display of a screen saver, brightness, backlight timeout, contrast, silent mode, office hours, power saving, and screen capture. Figure 2-37 shows sample device settings.

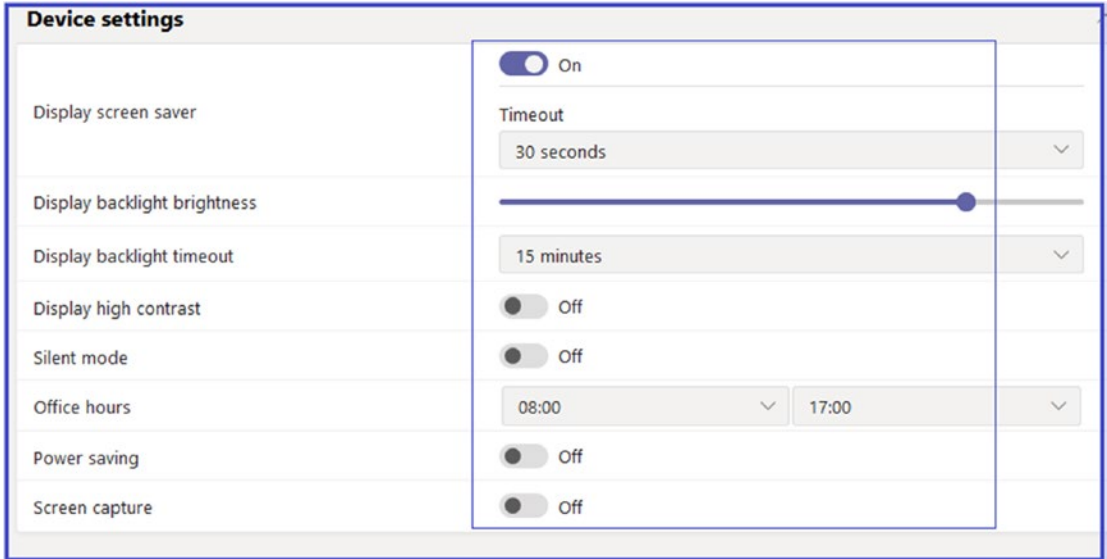


Figure 2-37. Device settings

- c. 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 2-38 shows a sample profile configuration with network settings.

Setting	Value
DHCP enabled	<input checked="" type="checkbox"/> On
Logging enabled	<input checked="" type="checkbox"/> On
Host name	Tracy
Domain name	bloguc.com
IP address	10.10.10.0
Subnet mask	255.255.255.0
Default gateway	10.10.10.1
Primary DNS	10.10.10.20
Secondary DNS	10.10.10.21
Device's default admin password	123456
Network PC port	<input type="checkbox"/> Off

Save Cancel

Figure 2-38. 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 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 2-39), 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 2-39 shows assignment of the configuration profile to a phone device.

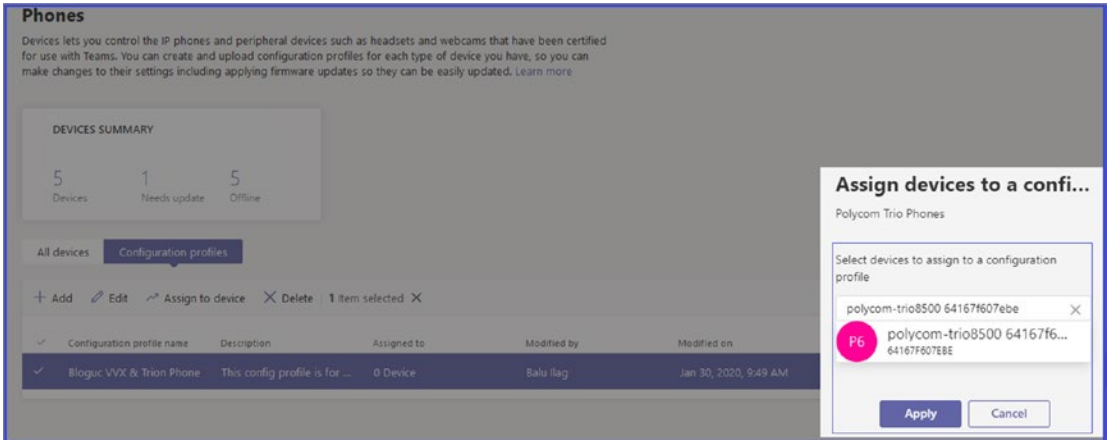


Figure 2-39. Assign configuration profile to a device

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 like updating phones, restarting phones for maintenance, and monitoring and diagnostics. You can also create and assign configuration profiles. Figure 2-40 shows the available management options.

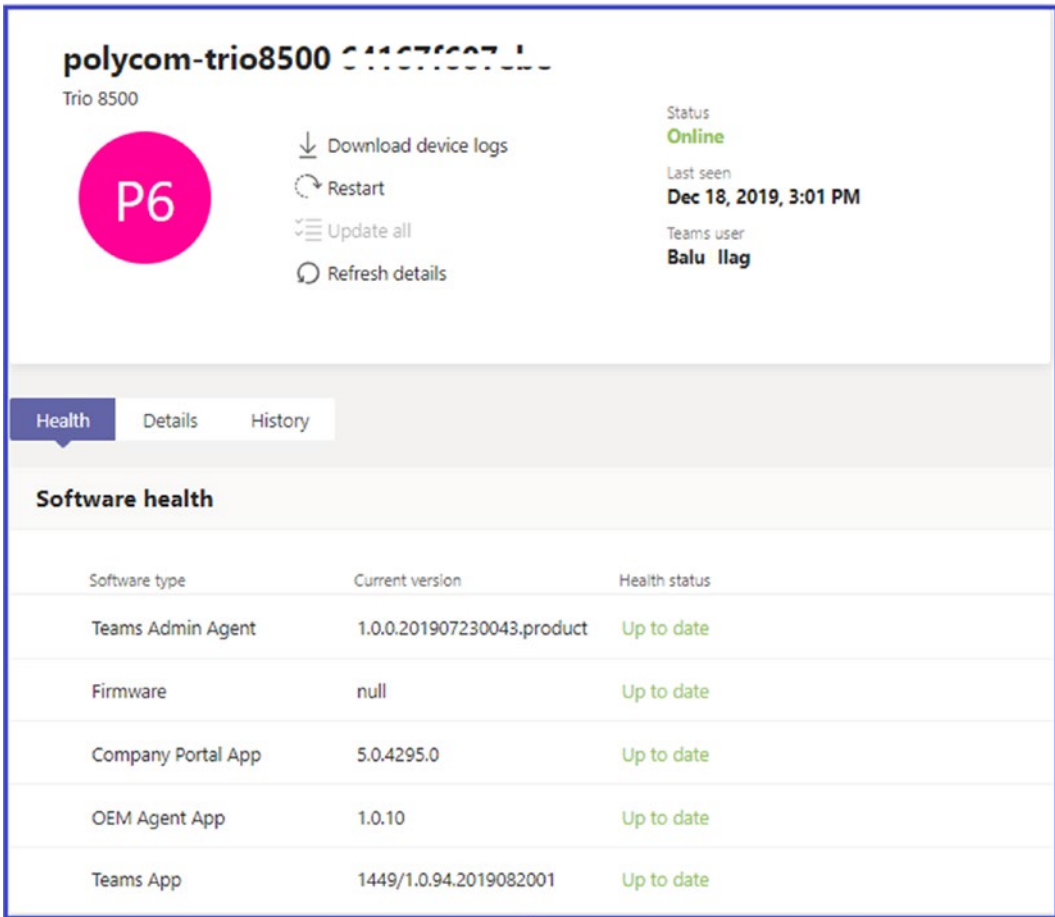


Figure 2-40. Phone management options

Configuring and Managing Microsoft Teams Rooms

Managing Microsoft Teams Rooms

Before configuring a Microsoft Teams Rooms 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 Microsoft Teams Rooms.

It is best practice to make sure to have plan for monitoring, administration, and management tasks on an ongoing basis. It is very 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 Microsoft Teams Rooms and which helpdesk queue will handle calls regarding Teams Rooms. As part of Teams room management, important administrative considerations include the following.

1. As an admin, have a proper plan for managing and configuring the local accounts that are created by the Microsoft Teams Rooms application installer.
2. You can consider using Microsoft Azure Monitor to monitor the Microsoft Teams Rooms deployment and report on availability, hardware and software errors, and Microsoft Teams Rooms application version. As of this writing, this monitoring facility is not available, but Microsoft plans to provide such monitoring in the future.
3. An additional consideration is whether the Teams 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. I would 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 Microsoft Teams Rooms 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 [77].

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

There are several best practices to adopt when managing Teams 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 very important because users will see it when searching for and adding Microsoft Teams Rooms systems to their meetings. As an example, you could use 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 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 Skype 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 [77].

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 call quality using the call quality dashboard.

Admin Center: Locations Tab

In 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 service like Enhanced 911. Network topology itself offers 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.

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 Teams admin center, then navigate to Locations and select Reporting Labels. Next, click Upload Locations Data, as shown in Figure 2-41.

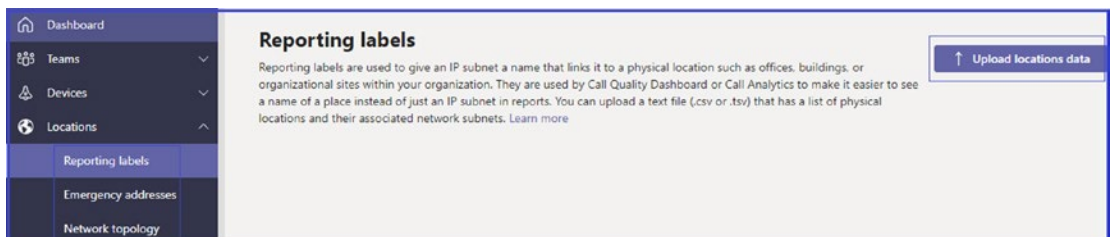


Figure 2-41. Upload Locations Data option

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 would recommend downloading the existing template and then updating it and uploading it so that you will see any error while uploading the file. Figure 2-42 shows the reporting label upload options.

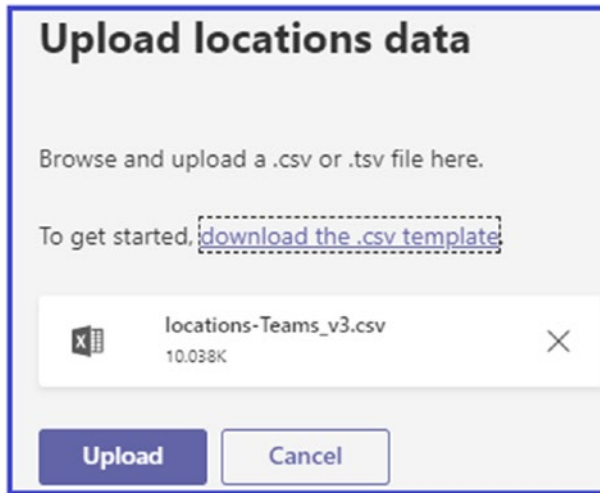


Figure 2-42. Uploading reporting labels

Emergency Addresses

Updating emergency addresses is critical because the emergency services such as 911 service are dependent on the emergency addresses updated in 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, 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 [78].

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 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 2-43 shows the Bloguc HQ office address.

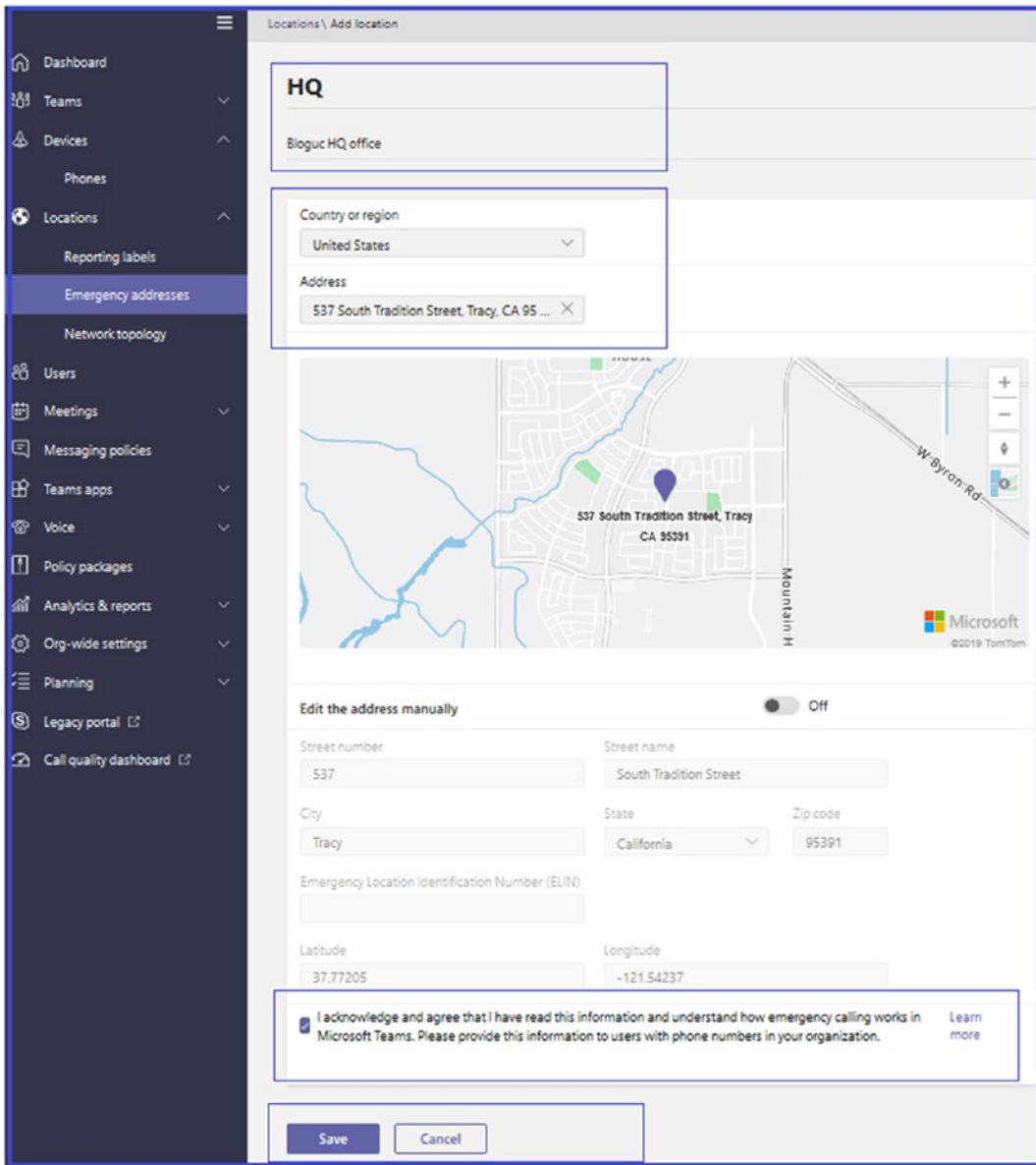


Figure 2-43. *Updating emergency addresses*

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 2-44 shows the Bloguc HQ office address and its validation status.

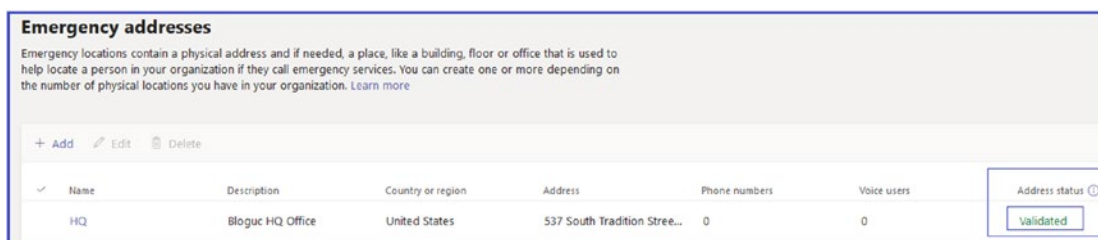


Figure 2-44. Emergency address added and validated

Note You can only change the address information for a location 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 that 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 that you want to remove from the list of locations, and then click Delete [78].

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 IPs 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 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, then set whether location based routing is enabled for this site or not. Select an emergency location, and finally click New to add the subnet. Figure 2-45 illustrates adding a network site.

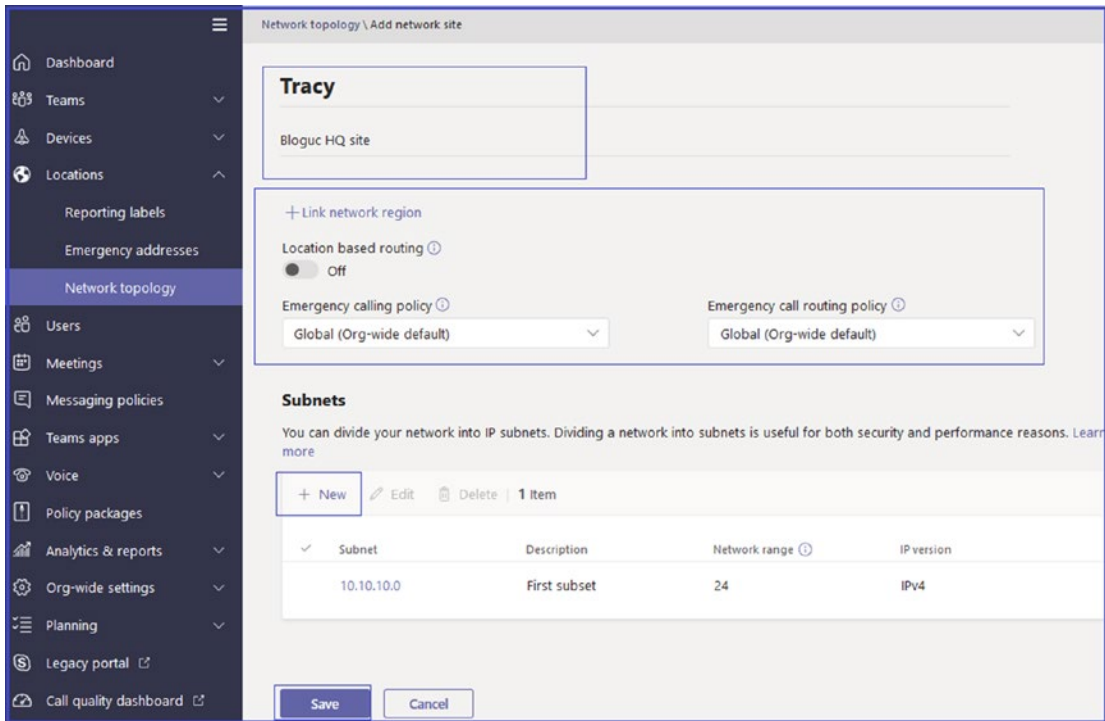


Figure 2-45. Network site

Click + *New* to add a new subnet with subnet mask and IP version (see Figure 2-46).



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 2-46. 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 IPs 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 2-47. Trusted IP addresses are required to implement 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.

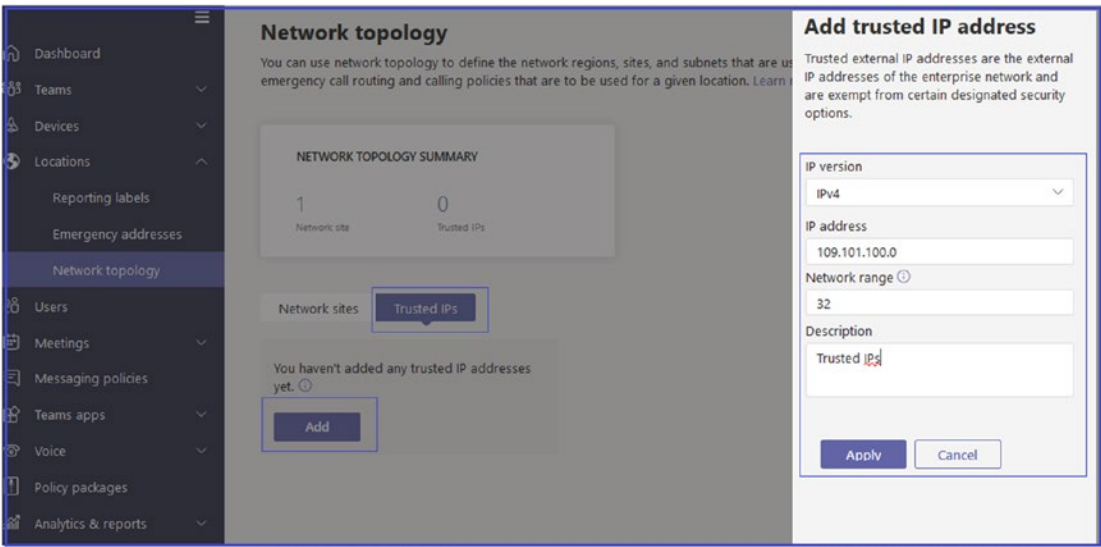


Figure 2-47. Adding a trusted IP

Admin Center: Users Tab

As an admin, most of your time will be spent managing users. In 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 and Skype for Business. Figure 2-48 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 Office 365 Admin center and navigate to Users.

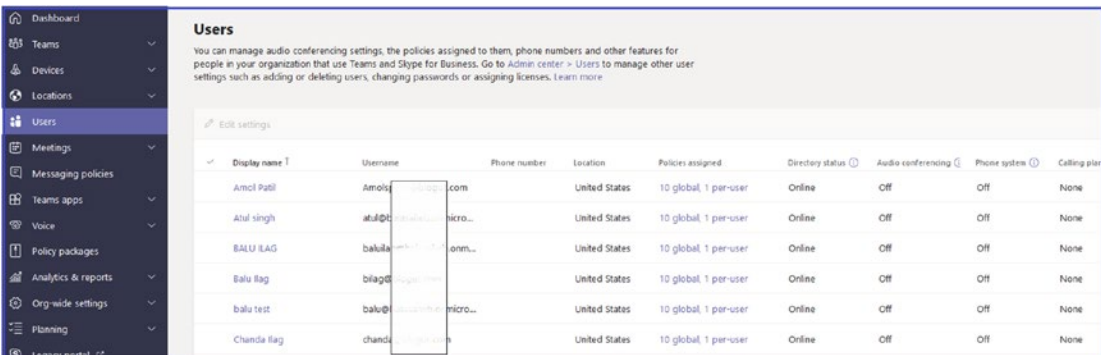


Figure 2-48. Users and their different settings

Admin Center: Meetings Tab

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, I 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 landline 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 very important for you as an admin to review and confirm that your environment is properly configured to provide your users the best possible experience.

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 that 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 four sections: General, Audio & Video, Content Sharing, and Participants & Guests. 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 General section, select whether to turn the following options on or off.
 - *Allow Meet Now In Channels:* This option allows users to host a meeting in a team channel.

- *Allow The Outlook Add-In:* This option is important because users can schedule Teams meetings through Outlook.
- *Allow Channel Meeting Scheduling:* This feature allows users to schedule channel meetings.
- *Allow Scheduling Private Meetings:* This feature allows users to schedule private meetings.

Figure 2-49 shows all of those options turned on in the General section.

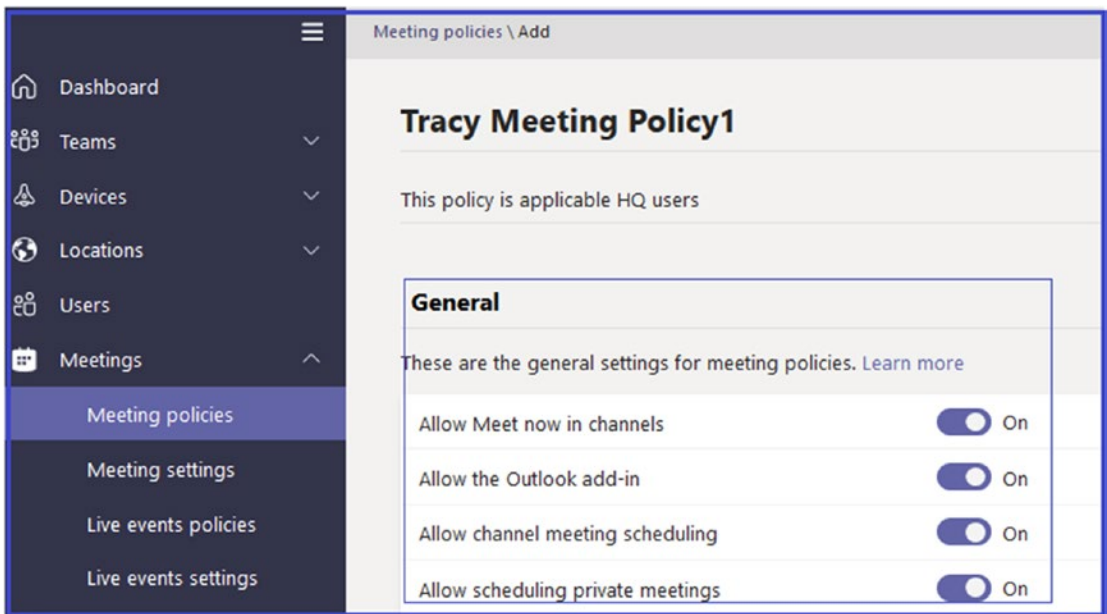


Figure 2-49. Setting meeting policies

For example, Allow Meet Now is a policy 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.

3. In the Audio & Video section, turn the following options on or off.
 - *Allow Transcription:* You can turn on or off transcription for a meeting.
 - *Allow Cloud Recording:* This is a popular feature that most users like.
 - *Allow IP Video:* You can also enter the media bit rate in KBs. This setting determines the media bit rate for audio, video, and video-based app sharing in meetings.

Figure 2-50 shows the Audio & Video meeting settings.

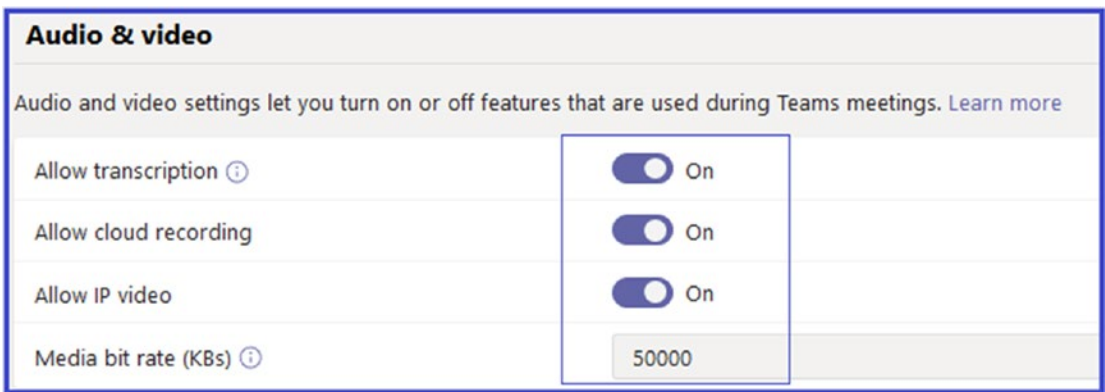


Figure 2-50. Audio & Video settings

For example, if the Allow Cloud Recording policy setting is turned on and the user is authenticated as a user from the same organization, then the recording can be started by the meeting organizer or by another meeting participant. This only concerns the internal users; guests do not have permission to start or stop a recording.

4. In the Content Sharing section, first select a screen sharing mode, such as Entire Screen, Single Application, or Disabled. Then turn the following options on or off.
 - Allow A Participant To Give Or Request Control
 - Allow An External Participant To Give Or Request Control
 - Allow PowerPoint Sharing

- Allow Whiteboard
- Allow Shared Notes

Figure 2-51 shows all available content sharing features.

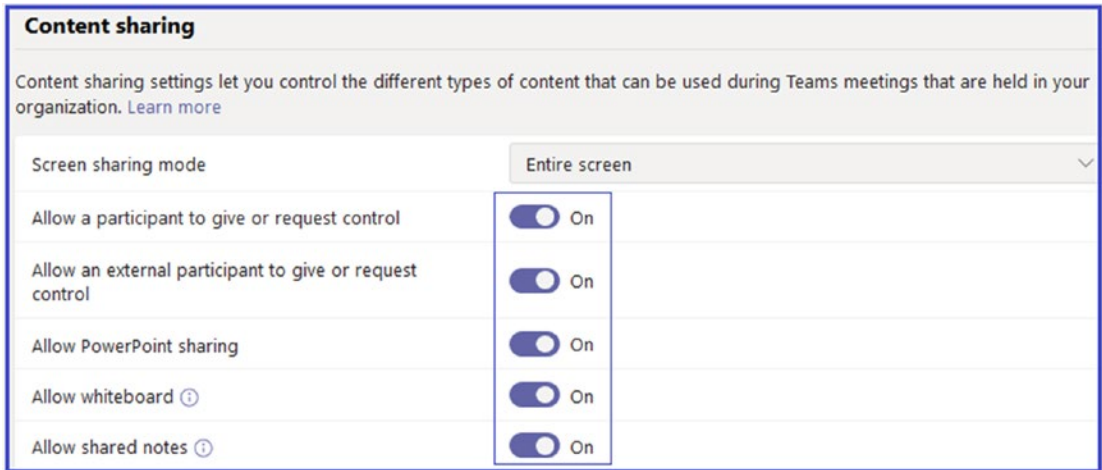


Figure 2-51. Content Sharing section

For example, the Allow A Participant To Give Or Request Control setting defines whether the user can give control of the shared desktop or window to other participants who are present in the meeting.

5. In the Participants & Guests section, you can elect to turn these options on or off.
 - Let Anonymous People Start A Meeting
 - Allow Dial-In Users To Bypass The Lobby
 - Allow Meet Now In Private Meetings

Make selections for the other feature options as well.

- *Automatically Admit People:* Select one of the following options:
 - Everyone
 - Everyone In Your Organization
 - Everyone In Your Organization And Federated Organizations

- *Enable live captions:* Select one of the following options:
 - Disabled But The Organizer Can Override
 - Disabled
- *Allow chat in meetings:* Select one of the following options:
 - Enabled
 - Disabled

Once you have finished entering your settings, click *Save* to commit the changes. Figure 2-52 shows all the recommended feature selections.

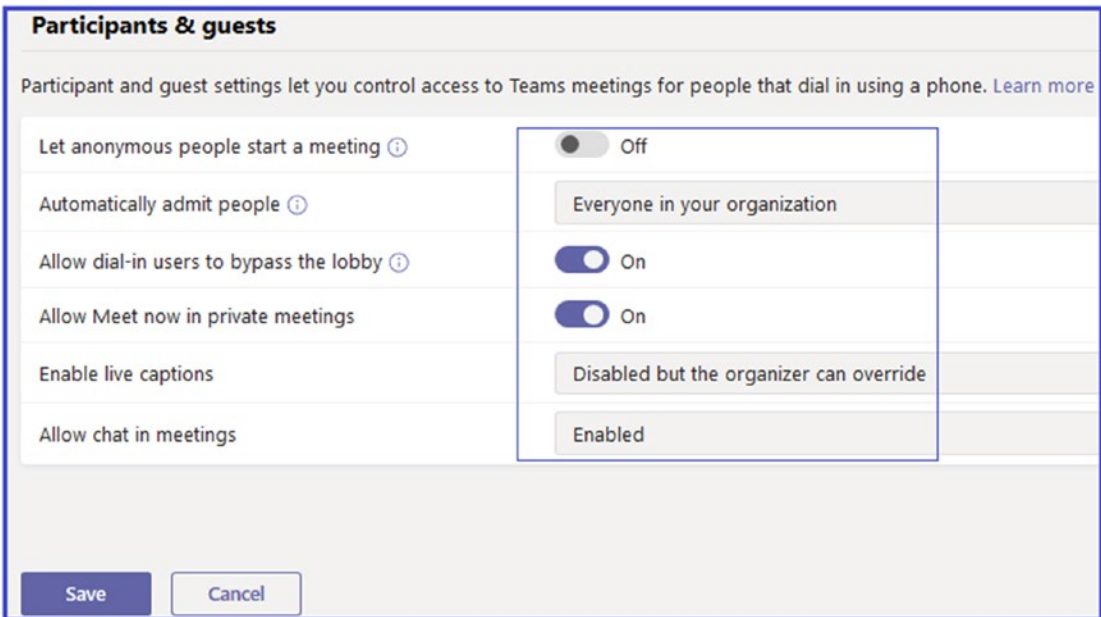


Figure 2-52. *Participants & Guests features*

As another example, if you turn off Allow Channel Meeting Scheduling, then the Schedule A Meeting option will not be available to users when they start a meeting in a Teams channel, and the Select A Channel To Meet option will not be available to users when they schedule a meeting from Calendar in Teams.

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 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.

1. To assign a policy using the Meeting Policies tab, simply log in to Teams admin center, then navigate to Meetings and select Meeting Policies. Select the required meeting policy and then click Manage Users. In the Manage users window, begin to enter a username. Once the full username shows, click Add and then click Apply to apply the policy. Figure 2-53 shows user Chanda Ilag added to the applied policy.

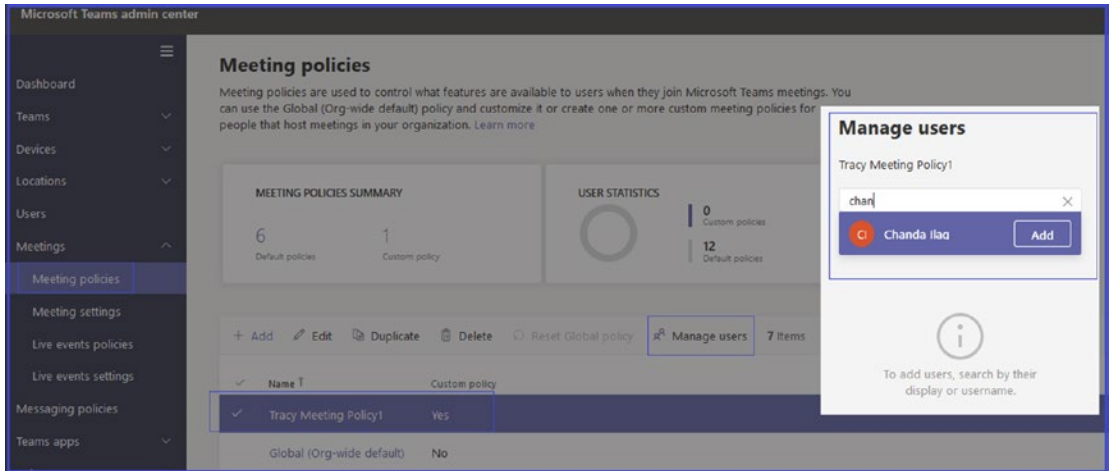


Figure 2-53. Policy assigned to user

2. To assign a policy using the Users section in Teams admin center, log in to Teams admin center, then navigate to Users. Select the users to whom you want to apply the policy and then click Edit. Under Edit User Policies, select the required meeting policy, and then click Apply, as shown in Figure 2-54.

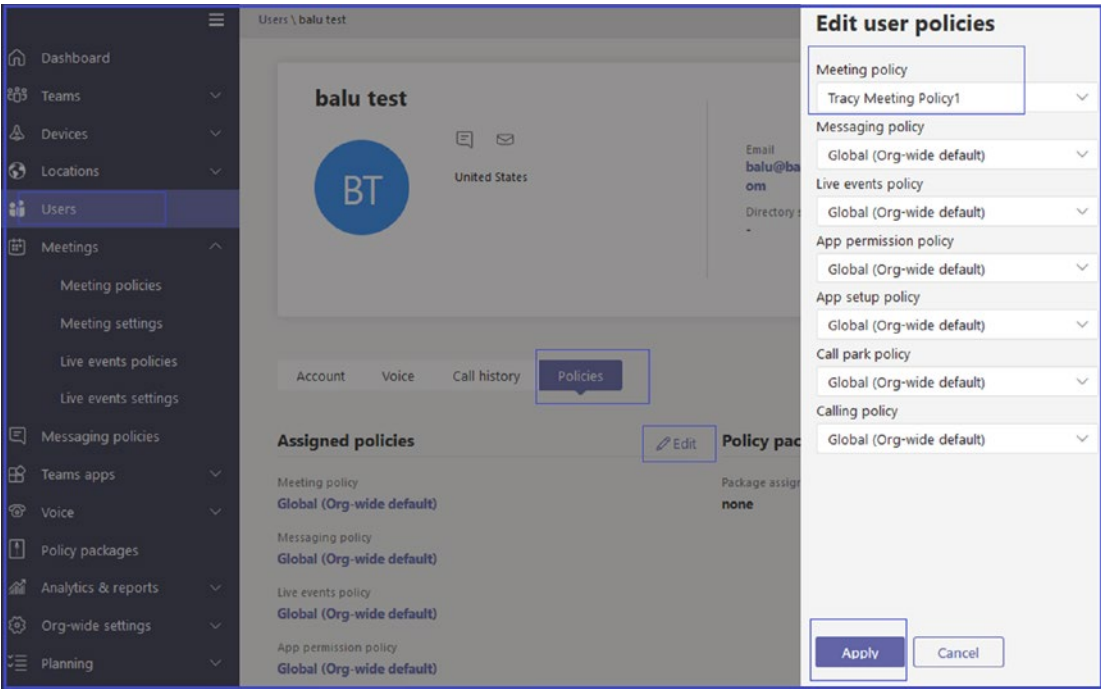


Figure 2-54. Assigning policies from the Users tab

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 postmeeting 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
```

Managing Meeting Settings

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 as per organization requirements. To enable anonymous users to join a meeting, log in to Teams admin center and navigate to Meetings. Select Meeting Settings, and under Participants, turn on the Anonymous Users Can Join A Meeting option. See Figure 2-55 for meeting settings.

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 applying 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 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 2-55 shows a preview for email invitation settings.

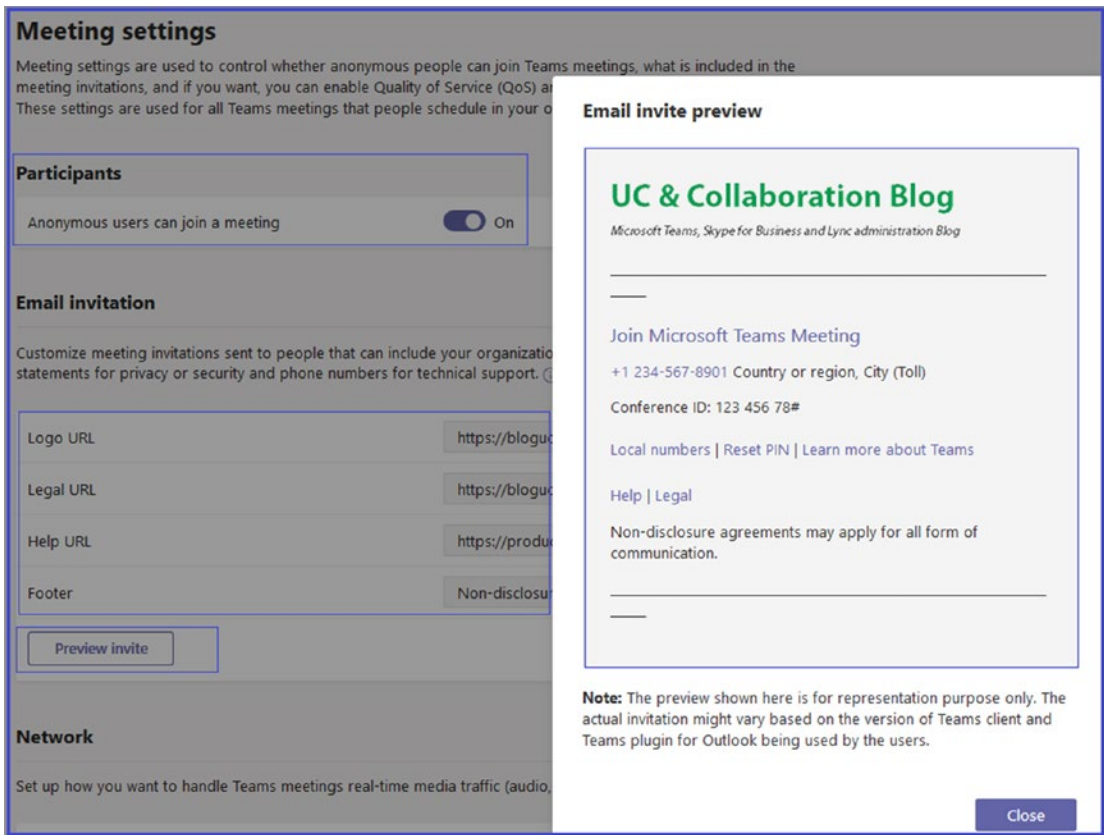


Figure 2-55. Email invitation customization

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 would recommend using the Specify Port Ranges option and using a smaller port range. Figure 2-56 shows all 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 2-56. QoS settings

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 possibility 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 any user can only be assigned to 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 Skype for Business Online PowerShell commands.

Note Any user can only have 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

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 Teams Admin Center. In the left-hand navigation pane, select Messaging Policies. Click + Add. On the top section in the 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 2-57 shows recommended settings, but the admin can customize the policy.

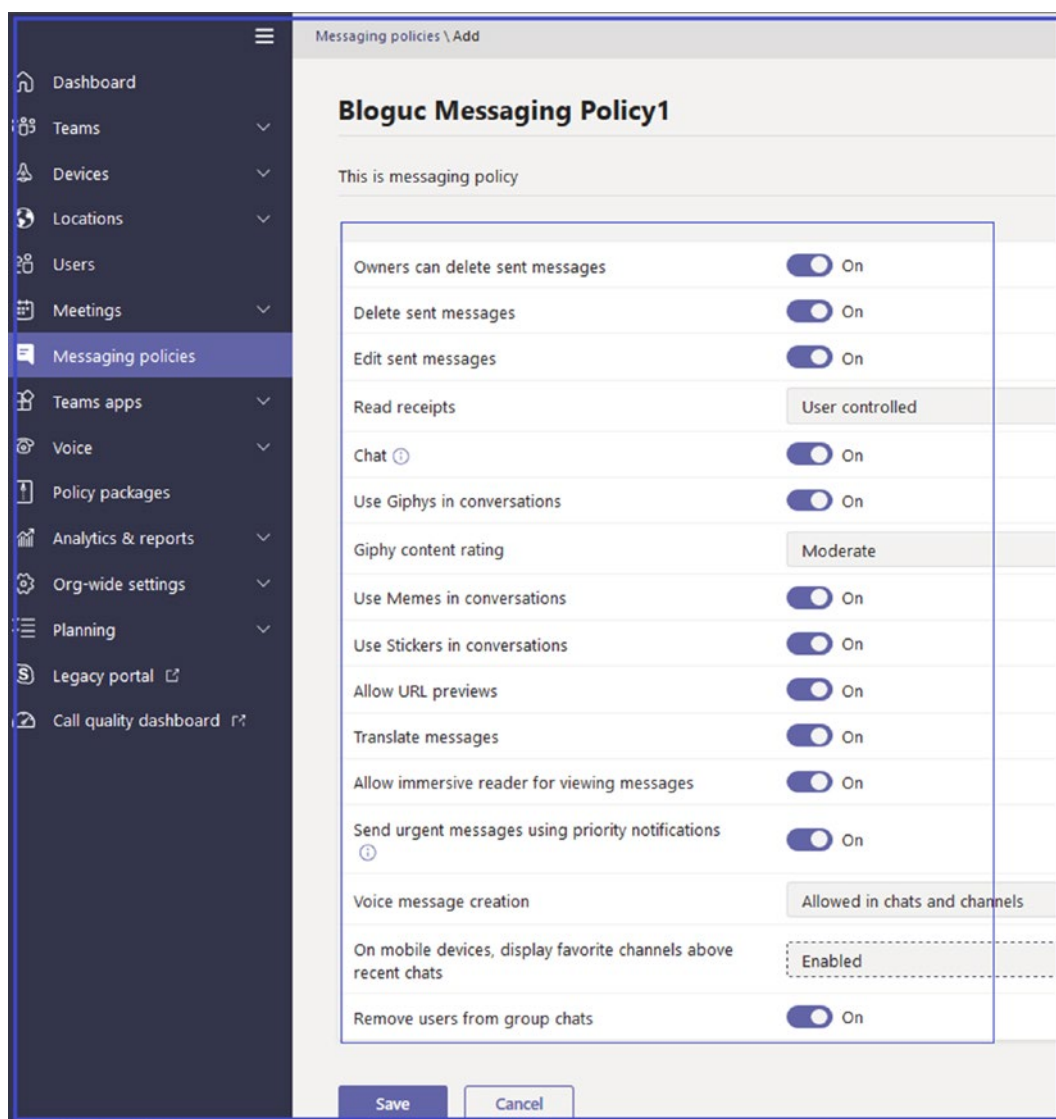


Figure 2-57. Messaging policy

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 Teams Admin Center, 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 2-58. The new messaging policy is now assigned to a user and its configured settings will be applied after up to 24 hours.

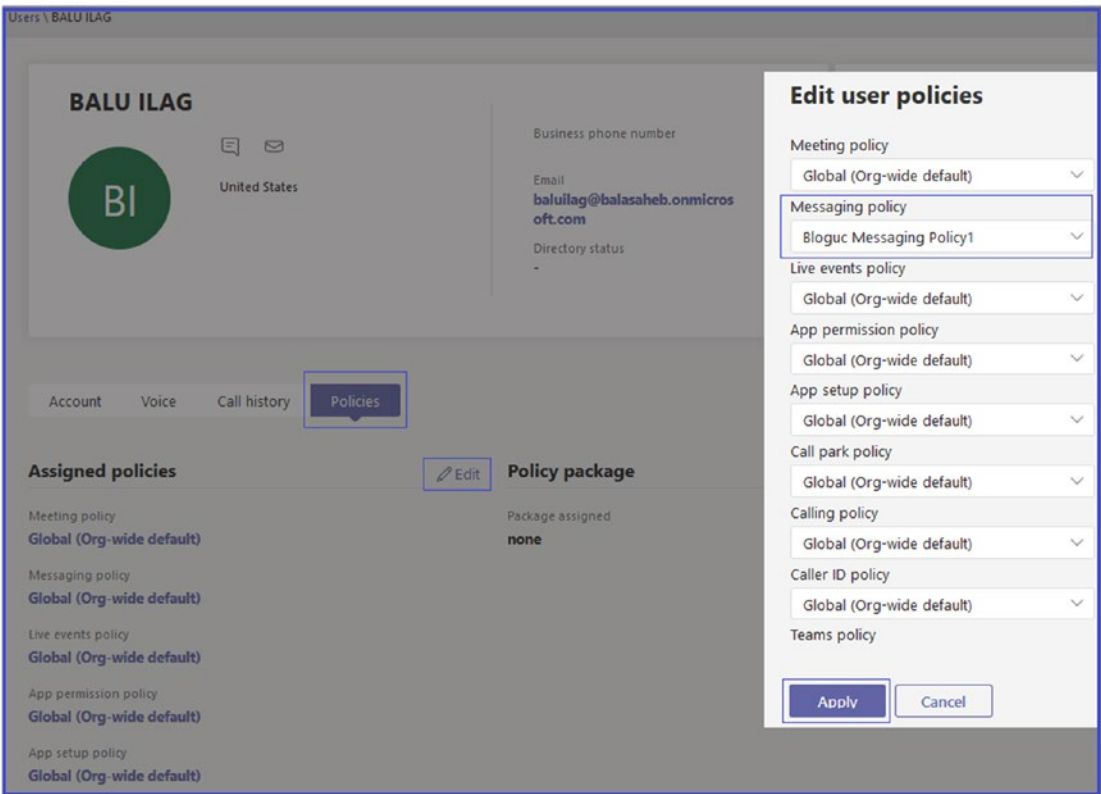


Figure 2-58. Messaging policy assigned to user

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 Teams Admin Center, then select Messaging Policies. Select the check box for the policy that you want to modify or delete. You should then select one of the following options, as shown in Figure 2-59:

- 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.

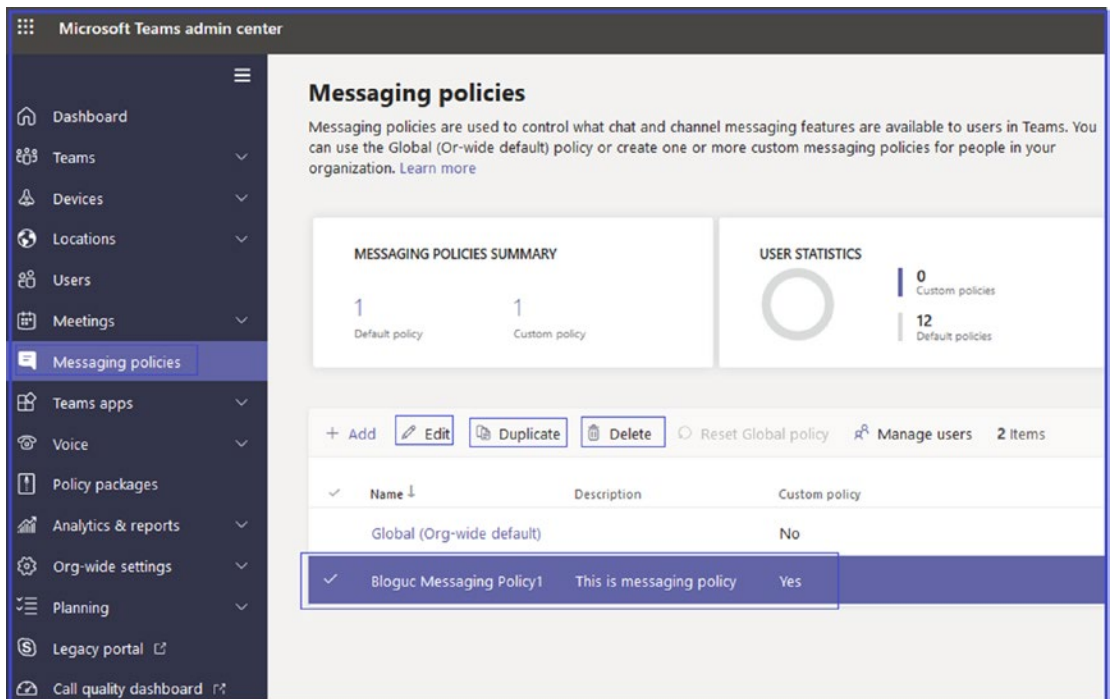


Figure 2-59. Modifying the messaging policy

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: Teams Apps Tab

In Teams admin center the next policy area is the Teams Apps tab. Microsoft Teams brings together all of the applications that end users use on a daily basis in one location. To manage applications as an admin is not difficult; however, you must know how to set up and assign policies.

Permission Policies

Microsoft Teams admin center has app Permission policies 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 design 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 assigned). Figure 2-60 shows the default policy.

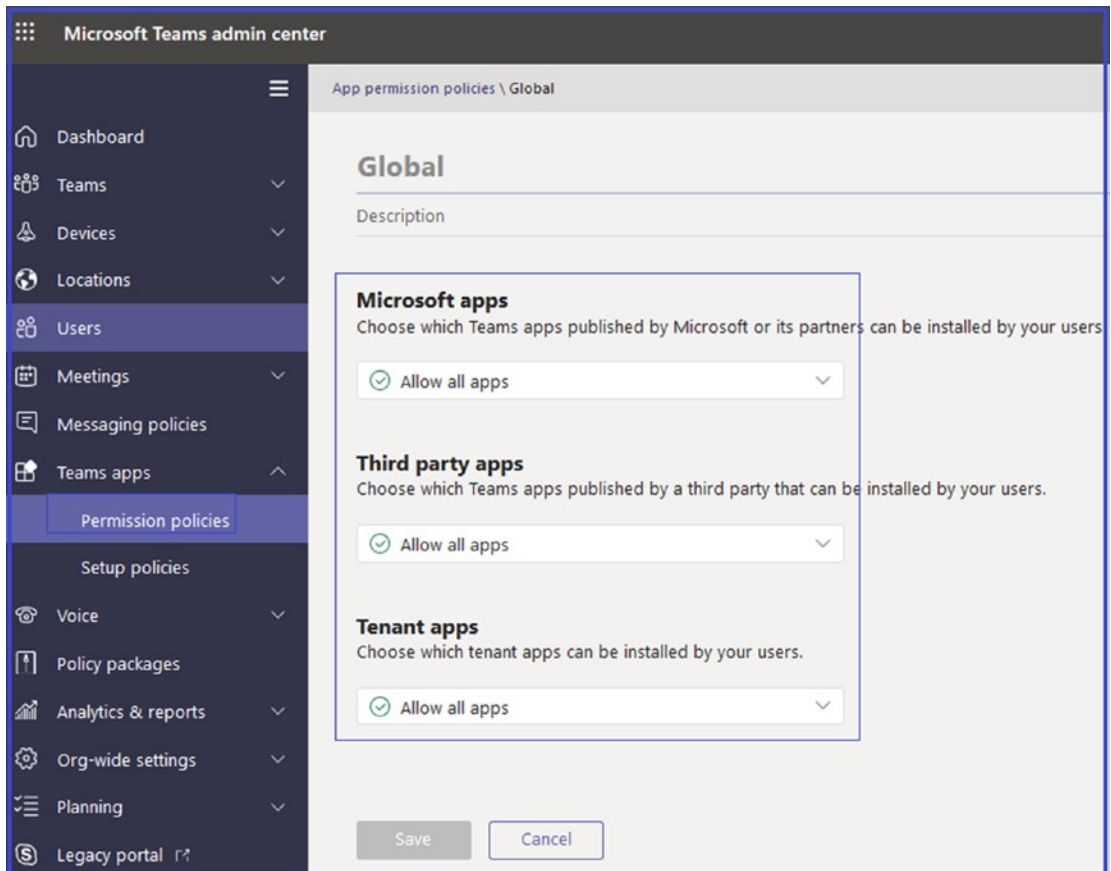


Figure 2-60. Teams global app permission policy

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 Teams admin center and navigate to Teams Apps and select Permission Policies. 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 2-61 shows all third-party apps and custom apps are allowed, and no apps are blocked.

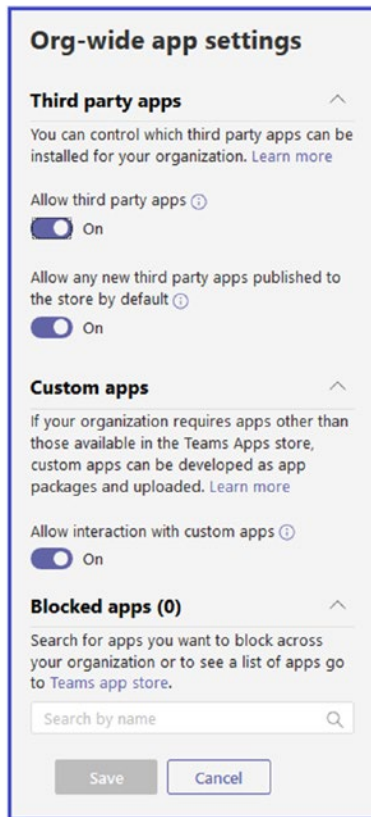


Figure 2-61. App Org-wide settings

Creating 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 Microsoft Teams admin center, and then navigate to Teams Apps. Select Permission Policies 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 2-62. You then have to add the apps that you want to allow.

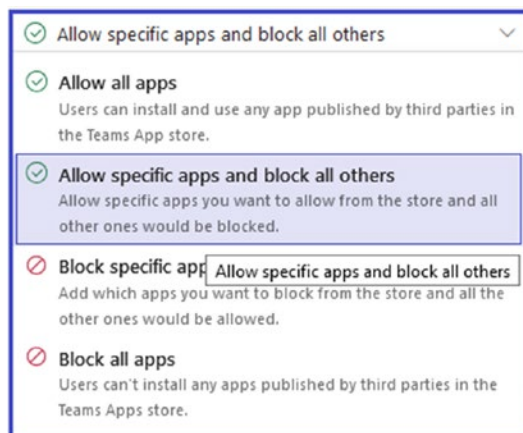


Figure 2-62. Allowing specific apps and blocking all others

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 2-63 shows that Twitter apps are 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.
7. Click Save to save the app policy. For the example shown in Figure 2-63, the Bloguc organization requirement is to allow all Microsoft apps and custom apps but block all third-party apps except Twitter apps.

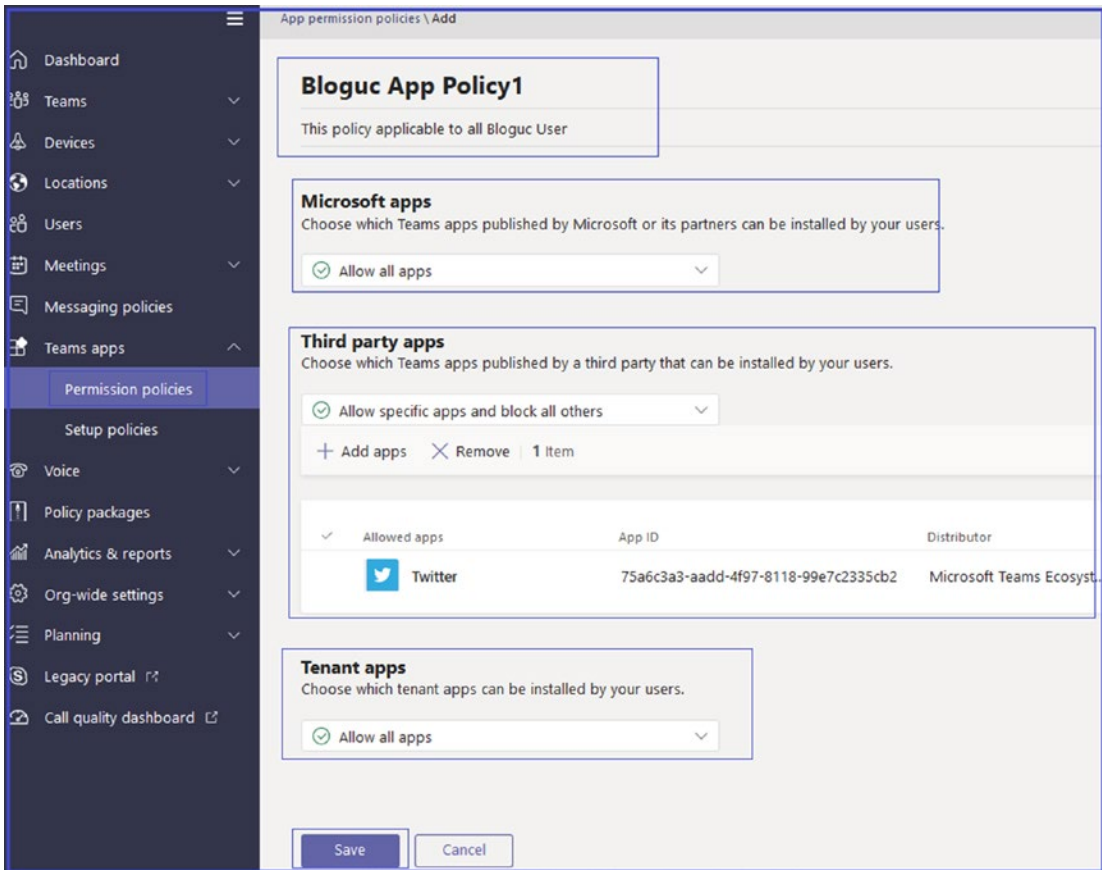


Figure 2-63. Teams app permission policy

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 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 2-64.

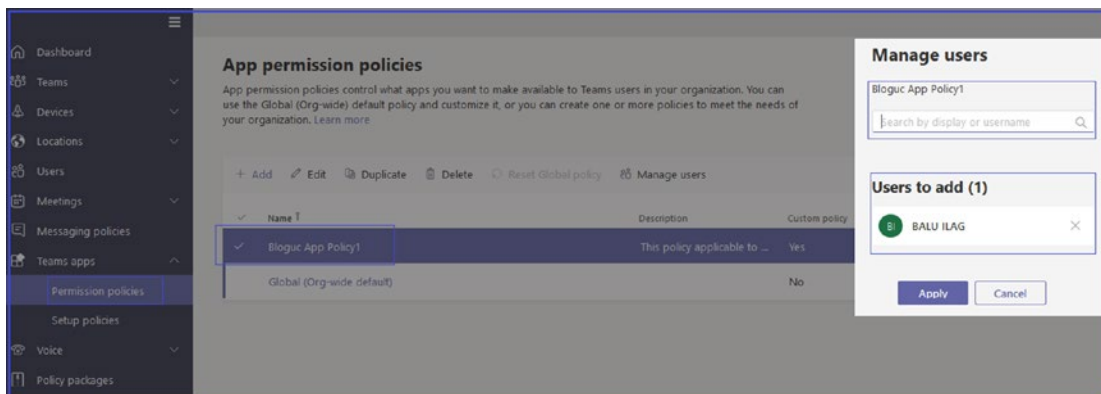


Figure 2-64. Assigning a policy to a user

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 Teams admin center. Simply log in to 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 thing is setup policies. 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 2-65 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.

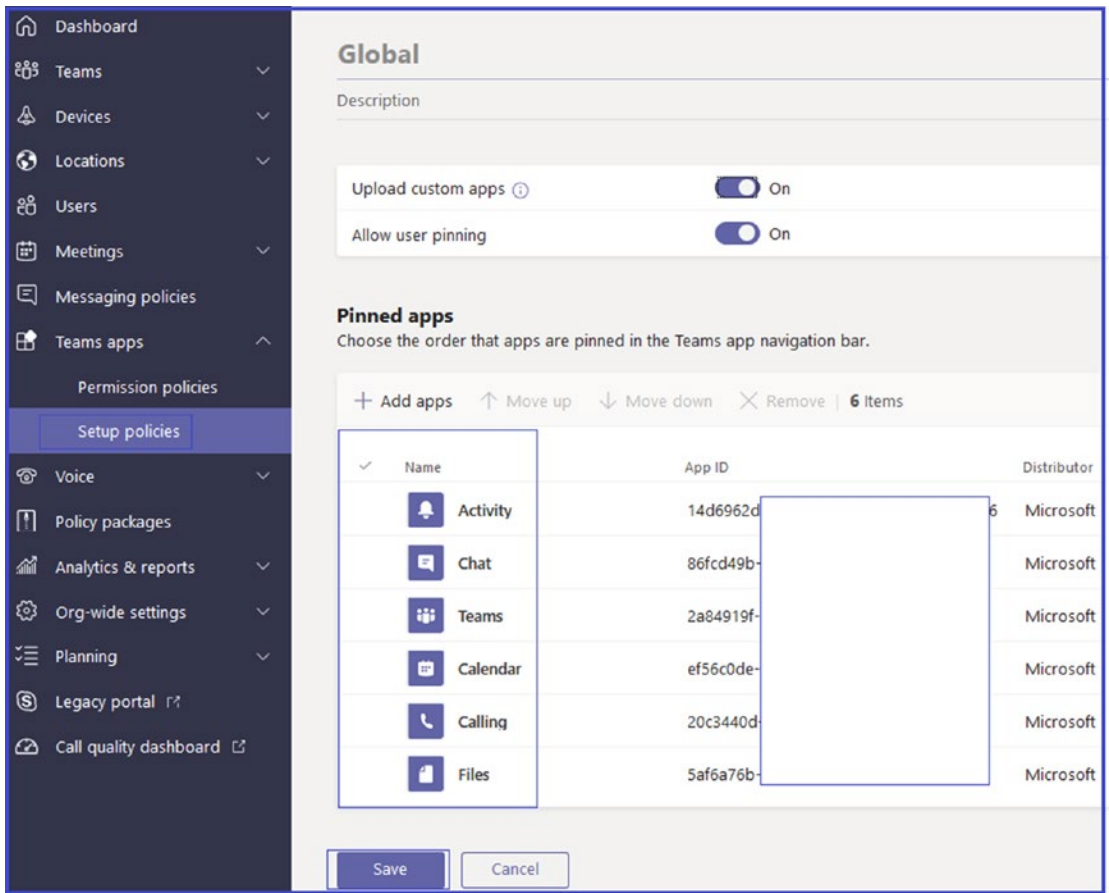


Figure 2-65. Setting setup policies

Figure 2-66 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.

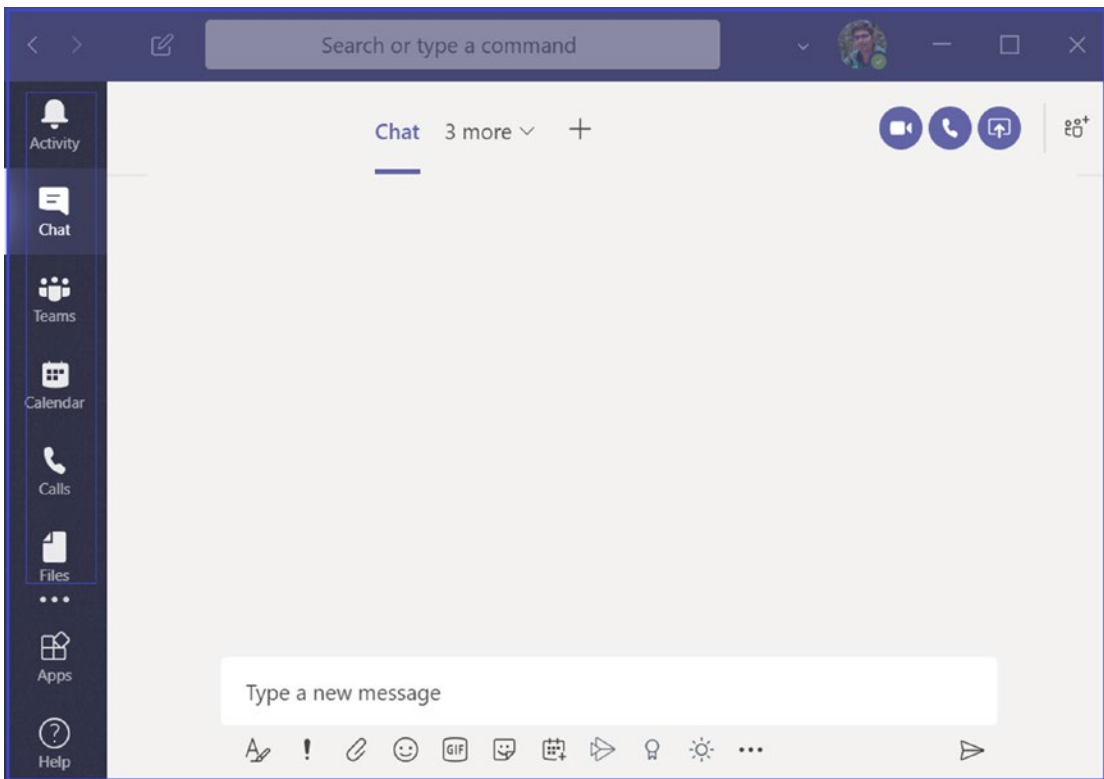


Figure 2-66. Teams apps set in a Teams setup policy

Managing the Teams Setup Policy

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, 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 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 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 Bloguc Organization wants to allow the Planner app, as shown in Figure 2-67.

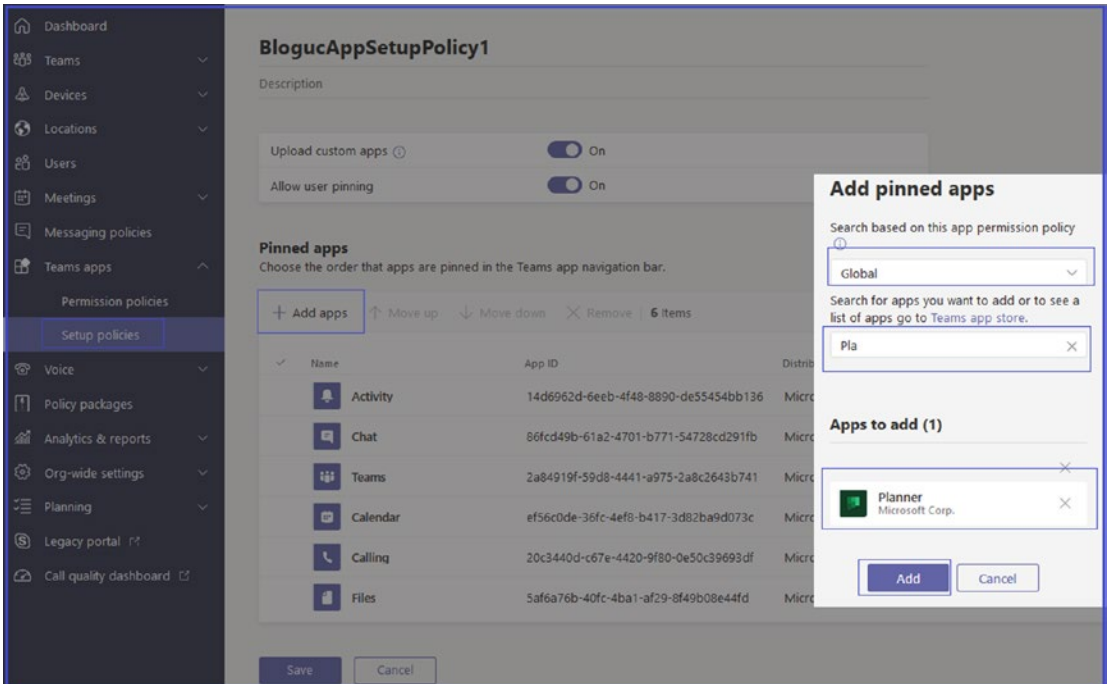


Figure 2-67. Adding apps to pinned apps

Once you click Add the Planner apps will be included under Pinned Apps, as shown in Figure 2-68.

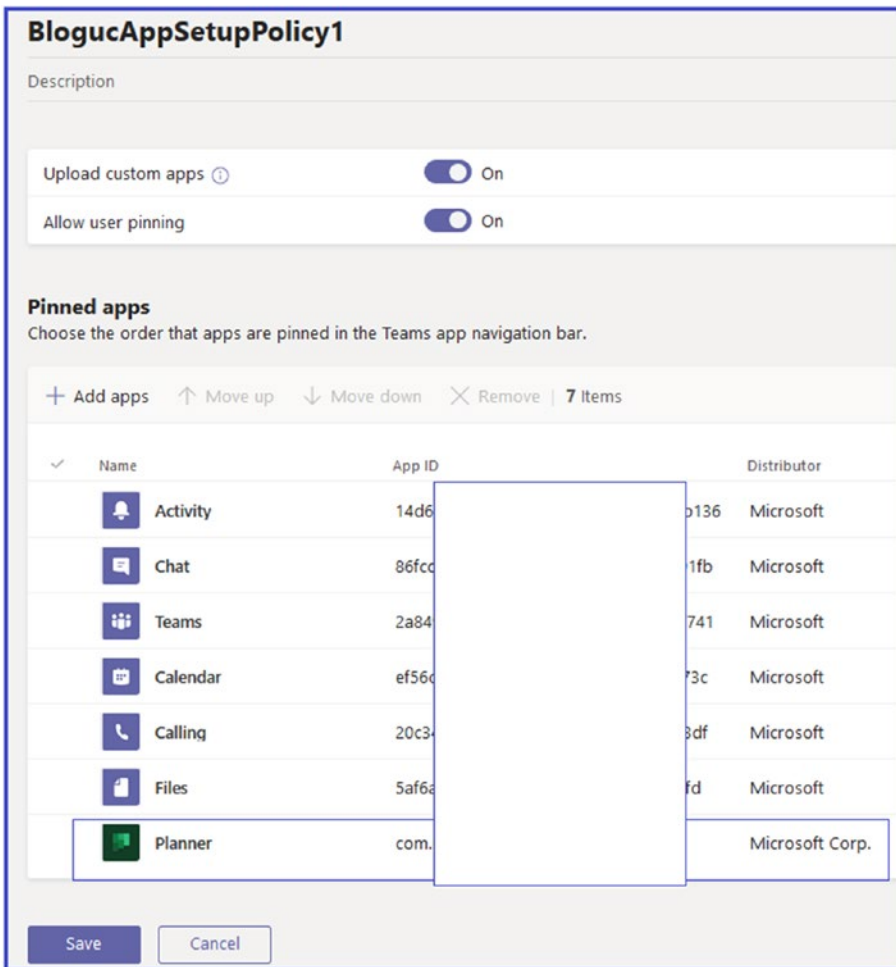


Figure 2-68. An app added to pinned apps

Assigning a Custom App Setup Policy to Users from 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 Teams admin center or PowerShell.

To assign policy using setup policies, in follow this procedure.

1. Log in to Teams admin center, then 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 that you want to add, as shown in Figure 2-69. Click Apply.

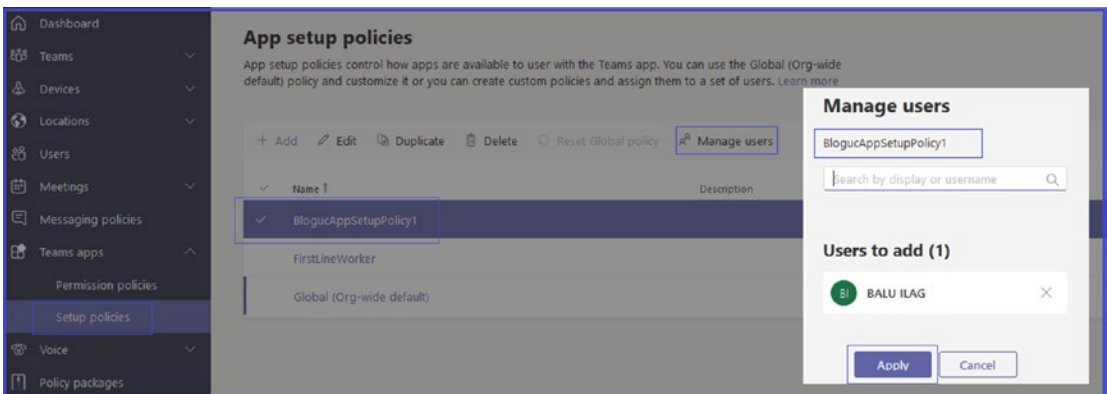


Figure 2-69. Assigning an app setup policy to a user

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 Teams admin center 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.

Admin Center: Voice Tab

The Voice tab includes several settings related to calling and phone usage for Microsoft Teams, as shown in Figure 2-70.

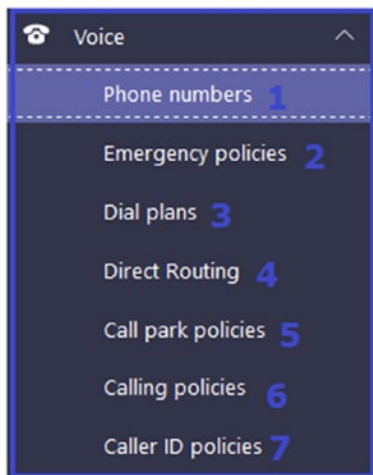


Figure 2-70. Voice features

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 like audio conferencing, auto attendants, or call queues.

Phone Number Management

Microsoft Teams admin center allows Teams IT admins to port their existing phone numbers, search for new numbers, and acquire new phone numbers from Office 365 Phone System (you might need to add using the legacy Skype for Business admin portal). 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 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 add a location first to search). Specify the quantity and then click Next. In the example shown in Figure 2-71, 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 5.

Note The number acquisition process takes some time, so be patient.

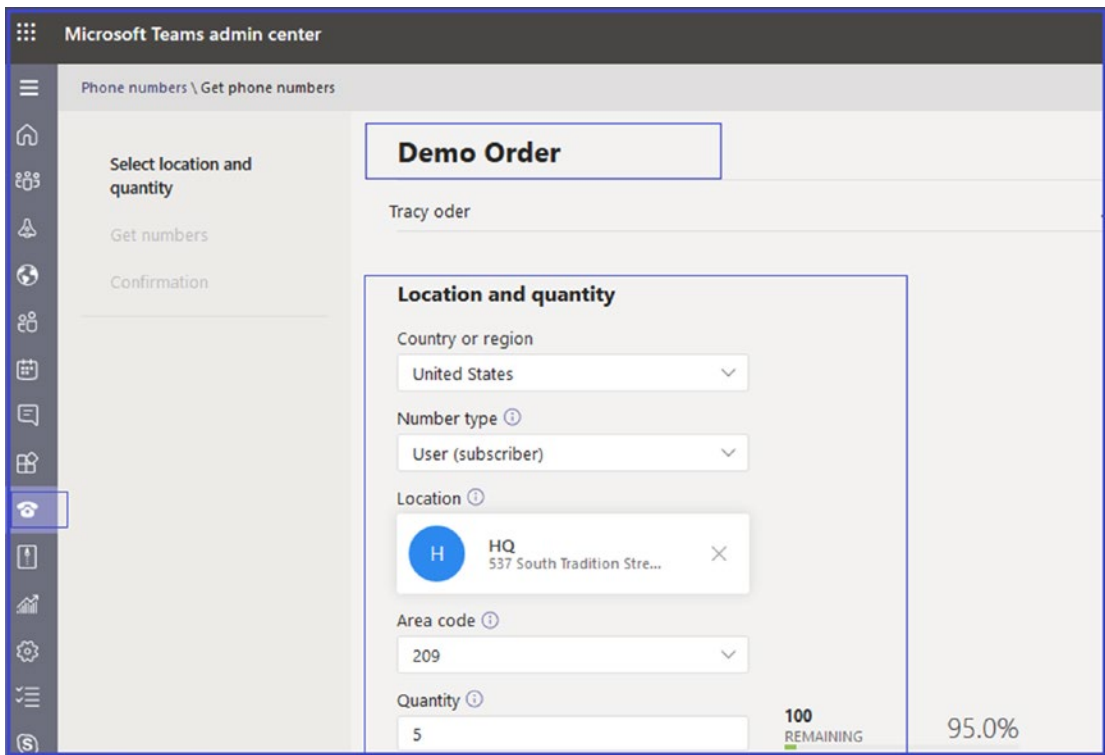


Figure 2-71. Phone numbers

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 Office 365 cloud. There are two processes for porting the phone numbers. as 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

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 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 2-72).

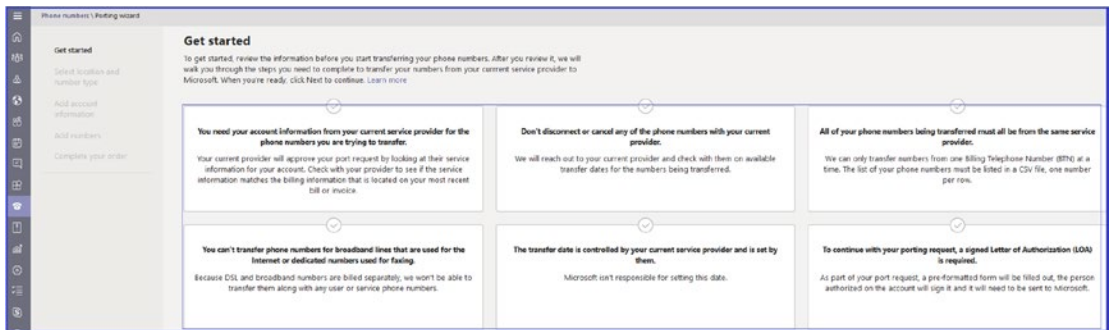


Figure 2-72. Porting the number

You can check the order history.

Emergency Policies

Emergency calling policies are used to control how users in your organization can use 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.

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 [79].

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

1. Log in to 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 2-73, 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 2-73 shows an example emergency calling policy.

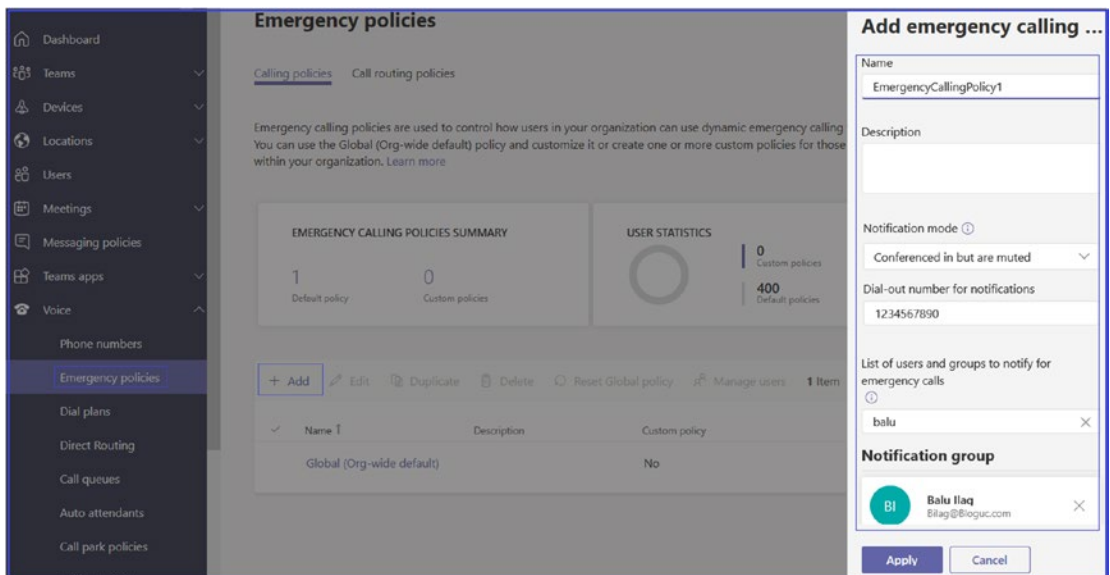


Figure 2-73. Emergency calling policy

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 Teams admin center or PowerShell.

Assigning an Emergency Calling Policy Using Teams Admin Center

Log in to 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 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 Skype for Business PowerShell module [79]. In this example, we assign a policy called Operations Emergency Calling Policy to all users in the Bloguc Security group.

Note Make sure you first connect to the Azure AD PowerShell for Graph module and Skype for Business PowerShell module by following the steps in Connect to all Office 365 services in a single PowerShell window. Connect-MsolService and Import-Module SkypeOnlineConnector *Creds = Get - CredentialsfbSession = New-CsOnlineSession -OverrideAdminDomain ".onmicrosoft.com" -Credential CredsImport - PSSessionsfbSession.*

```
$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 [80]. 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 Teams admin center as well PowerShell. To create an emergency call routing policy using Teams admin center, follow these steps.

1. Log in to 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 policy and location information from the service and includes that information as part of the emergency call. Figure 2-74 shows the enhanced emergency services enabled.

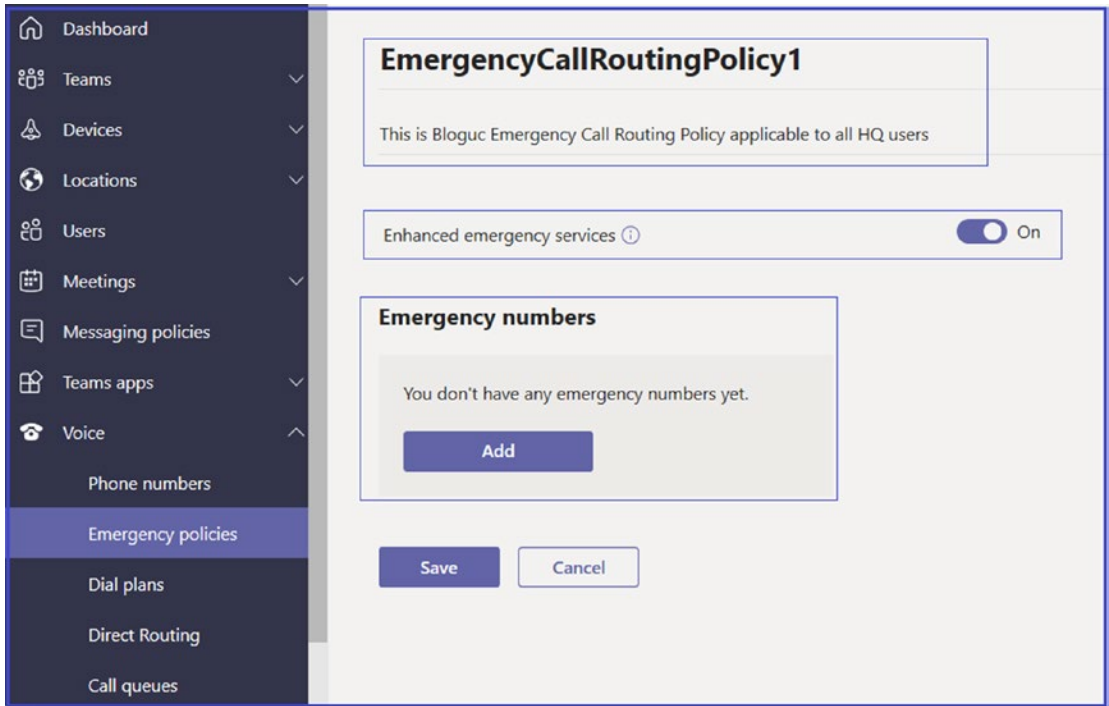


Figure 2-74. *Emergency call routing policy*

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 2-75, 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 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 2-75.
- 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 2-75.

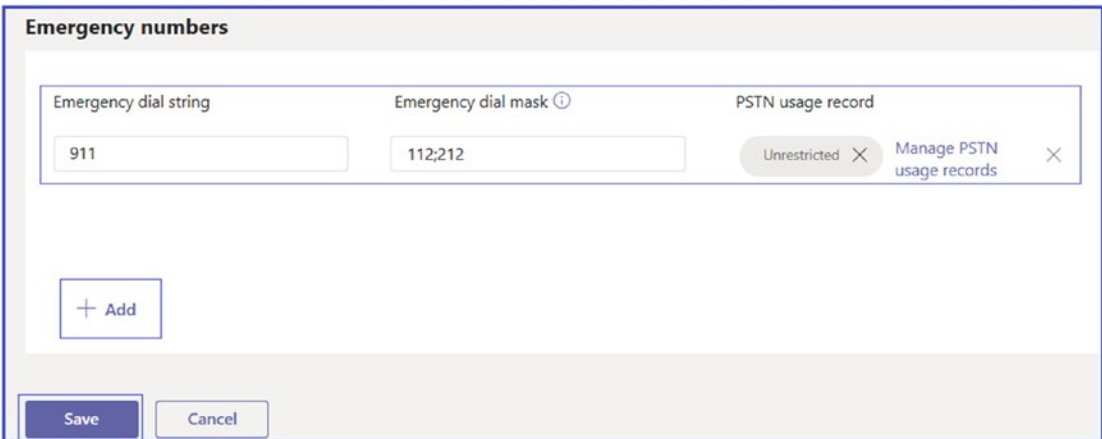


Figure 2-75. Emergency numbers

5. Once you are finished adding all emergency numbers, click Save. Remember, Figure 2-75 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.

Note For Direct Routing, Microsoft is transitioning away from Teams clients sending emergency calls with a “+” in front of the emergency dial string. Until the transition is completed, the voice route pattern to match an emergency dial string should ensure a match is made for strings that have and don’t have a preceding “+”, such as 911 and +911. For example, `^\+?911` or `.*`. [80]

Dial strings and dial masks must be unique within a policy. This means that for a policy, you can define multiple emergency numbers and you can set multiple dial masks for a dial string, but each dial string and dial mask must only be used one time. [80]

Assigning a Custom Emergency Call Routing Policy to Users Using Teams Admin Center and PowerShell

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

1. Log in to Teams admin center, and then navigate to Users. Select the user and then click Policies. and
2. Under Assigned Policies, click Edit.
3. Under Emergency Call Routing Policy, select the policy you want to assign (e.g., EmergencyCallRoutingPolicy1), 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 Skype for Business 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.

```
$members | ForEach-Object { Grant-CsTeamsEmergencyCallRoutingPolicy
-PolicyName "EmergencyCallRoutingPolicy1" -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
"Emergency Call Routing Policy 1"
```

Dial Plans

Dial plans provide a method for admins to configure the way end users can dial phone numbers and have them converted into E.164 format (globally accepted format) for routing. Microsoft Teams gives the ability to have custom dial plans that are essentially a collection of normalization rules that are used to translate a user's dialing behavior into something that can be routed on PSTN. In Teams the dial plan has been there, but it never had an interface to configure it using either the Skype for Business admin center or in the Microsoft Teams admin center. Traditionally this was all performed in PowerShell using the `CsTenantDialPlan` cmdlet object by prioritizing multiple normalization rules through the `CsVoiceNormalizationRule` cmdlet object created in regular expression (RegEx). Basically, regular expression 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 2-76 shows a default dial plan.

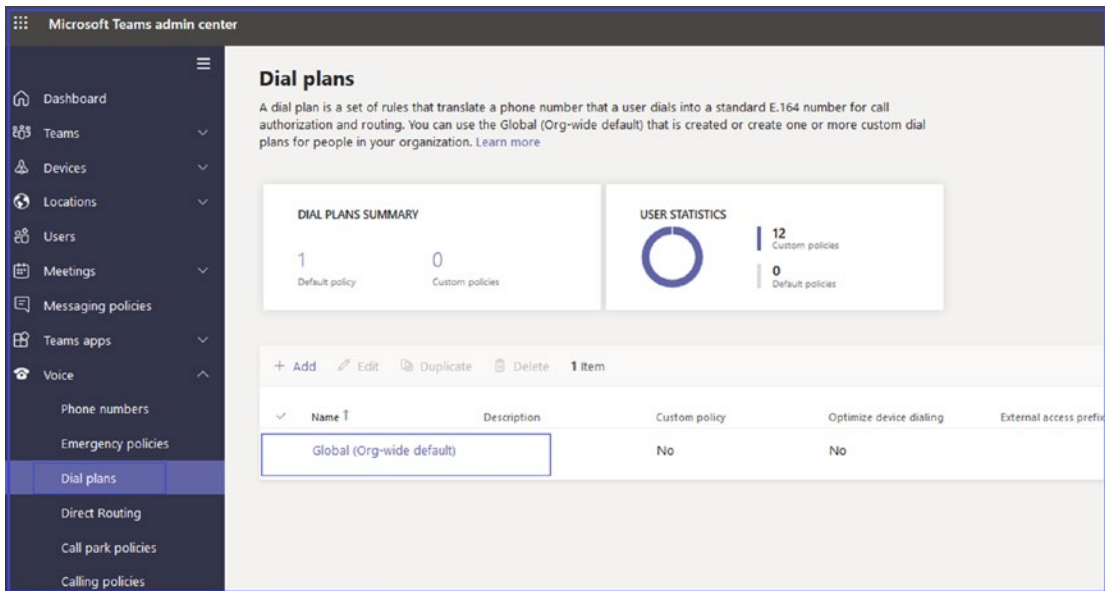


Figure 2-76. Default dial plan policy

Creating a Custom Dial Plan

To create custom dial plan, follow this procedure.

1. Log in to Teams admin center, 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 2-77 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 2-77.

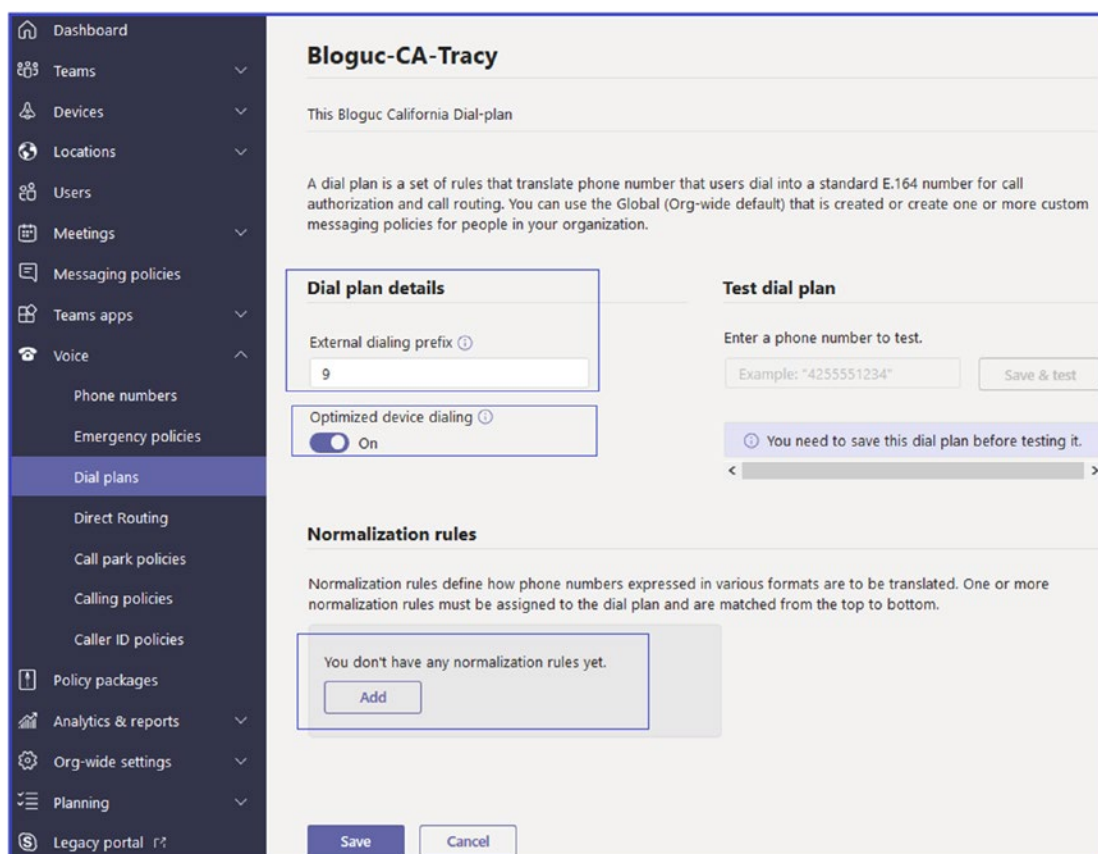


Figure 2-77. *Configuring a dial plan*

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 2-78 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 that 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 2-78 shows five digits tested to make sure it normalizes correctly with E.164 format. For example, here the result shows +12096566625.

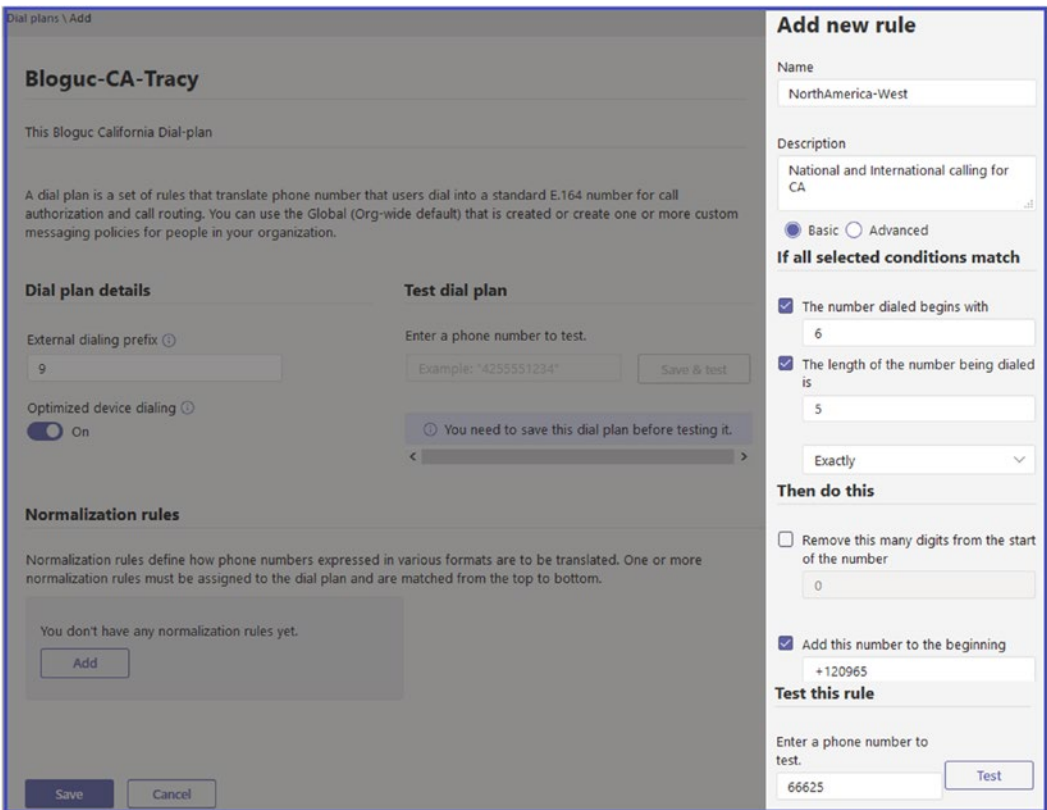


Figure 2-78. Normalization rule

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 very basic option for conditions without regular expression, and advanced for complex dial plans with multiple conditions using regular expression. Figure 2-79 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; for example, 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 2-79. 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 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 that you want to add. The example in Figure 2-80 shows assigning a dial plan to user Balu Ilag.

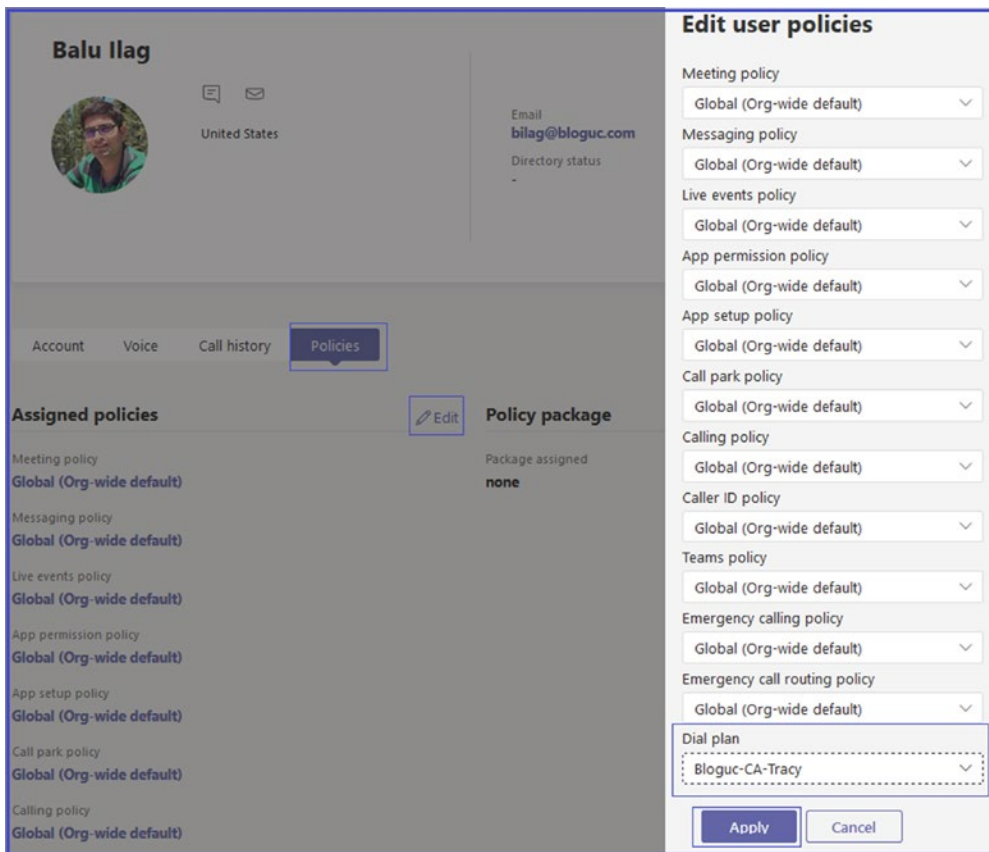


Figure 2-80. Assigning a dial plan to a user

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 Skype for Business Online tenant to the Office 365 organization. You must have Skype for Business Online PowerShell installed; you can use this link to download the Skype for Business Online PowerShell module: <https://go.microsoft.com/fwlink/p/?LinkId=532439>.

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

```
Import-Module skypeonlineconnector
$credential = Get-Credential
$session = New-CsOnlineSession -OverrideAdminDomain "<tenant name>.
onmicrosoft.com" -Credential $credential
Import-PSSession $session
```

For example, the domain name for my demo tenant is "bloguc.onmicrosoft.com".

After connecting to Skype for Business Online PowerShell, run the next command to create a new dial plan:

```
New-CsTenantDialPlan -Identity Bloguc-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"}
```

Direct Routing

Direct Routing allows the Teams admin to connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features (PSTN calls). For example, you can configure on-premises PSTN connectivity with an SBC to send and receive phone calls from a user with the Teams client. Direct routing 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., Bloguc Organization using Ribbon SBC to connect ATT SIP trunk), Direct Routing enables you to connect a supported SBC to 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 Microsoft Phone System [57].

Figure 2-81 shows the connectivity from on-premises PSTN connectivity with a Microsoft Teams client using Direct Routing capability.

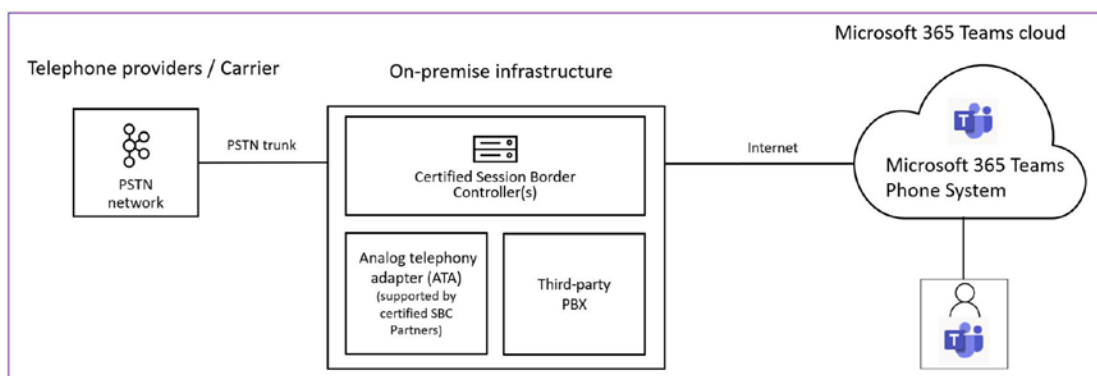


Figure 2-81. Teams Direct Routing high-level connectivity

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 Microsoft Phone System to enable voice calling features (PSTN calls). Direct Routing can be deployed in organizations who want to leverage on-premises PSTN within the following scenarios:

- Microsoft Calling Plan is not available in the organization's country or region. Thus far, Microsoft Calling Plan is available in only some countries only. 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 find the countries and regions where Calling Plan is available.

- The organization requires 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.

1. 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>.
2. 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 Microsoft Phone System through Direct Routing; for example, PSTN carrier ► SBC ► Microsoft Teams Office 365 Cloud.
3. You must have Office 365 Tenant where your organization's Teams users are located or homed.
4. 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.
5. 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.

6. 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.
7. 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.
8. 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. The 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

9. 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).

10. Specific to the Media traffic codecs 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:
 1. Non-media bypass (SBC to Cloud Media Processor): SILK, G.711, G.722, G.729
 2. Media bypass (SBC to Teams client): SILK, G.711, G.722, G.729, OPUS
11. 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.
12. 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 and Skype for Business Plan 2 (from Office 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 `New-CsOnlinePSTNGateway` only. There is no option to configure Direct Routing through the Team Admin center. Microsoft will be adding Direct Routing configuration capability for Teams admins in the Teams admin center portal to perform configuration of Direct Routing and

controlling 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 Skype for Business Online 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 [57a].

Let's configure Teams Direct Routing using Skype for Business Online PowerShell.

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

```
Import-Module skypeonlineconnector
$sfboSession = New-CsOnlineSession -OverrideAdminDomain
"domain.onmicrosoft.com"
Import-PSSession $sfboSession -AllowClobber
```

For example, my domain is `Bloguc.onmicrosoft.com`.

- b. After you are connected to Skype for Business Online 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
```

For 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 its 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 2-82 shows an example of PSTN gateway details.

```
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 2-82. 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 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 Skype for Business 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, Skype for Business Online, 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 Skype for Business 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 Online Voice routing policy available connect to Skype for Business online PowerShell and assign online voice routing policy to user. Refer below PowerShell command to assign 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 2-83 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.

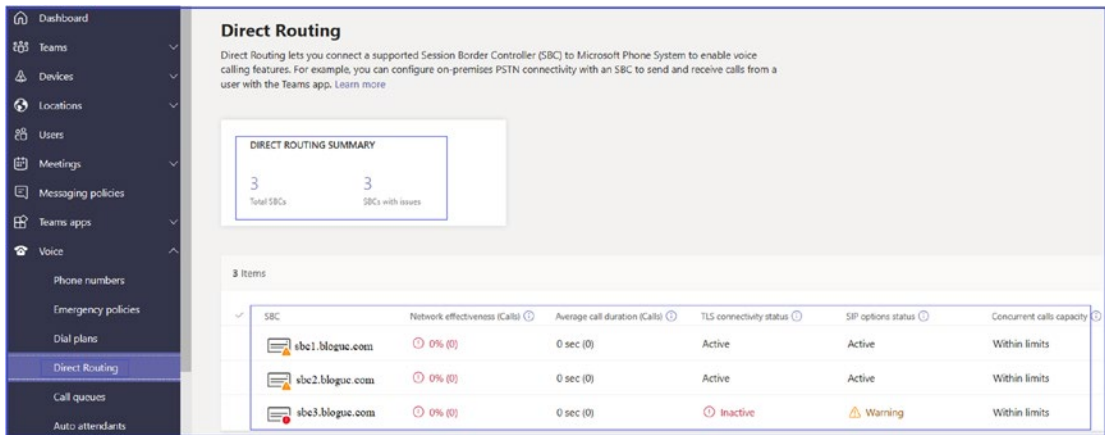


Figure 2-83. Teams Direct Routing dashboard

When you click on sbc1.bloguc.com, it shows the statistics regarding calls, network parameters, and concurrent calls happening through this SBC, as displayed in Figure 2-84.

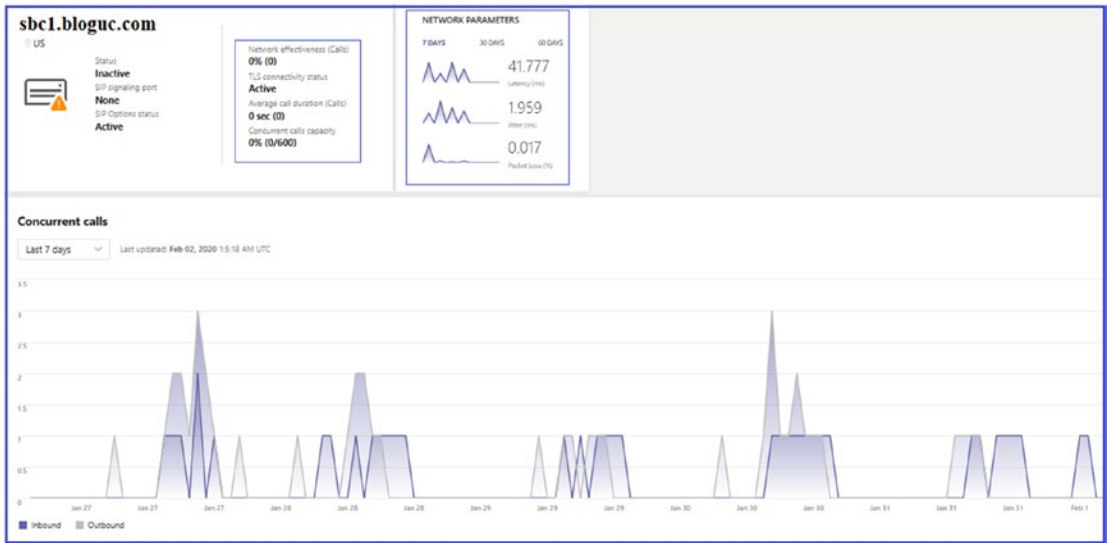


Figure 2-84. Teams Direct Routing SBC view

Call Park Policies

Call park 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.

Creating a Call Park Policy

To create a call park policy, you must have Teams service admin group permission. To do so, follow these steps.

1. Log in to Teams admin center then navigate to Voice. Select Call Park Policies.
2. Click + Add and then give the policy a name. Set the Allow Call Park option to On. Figure 2-85 shows an enabled call park policy.

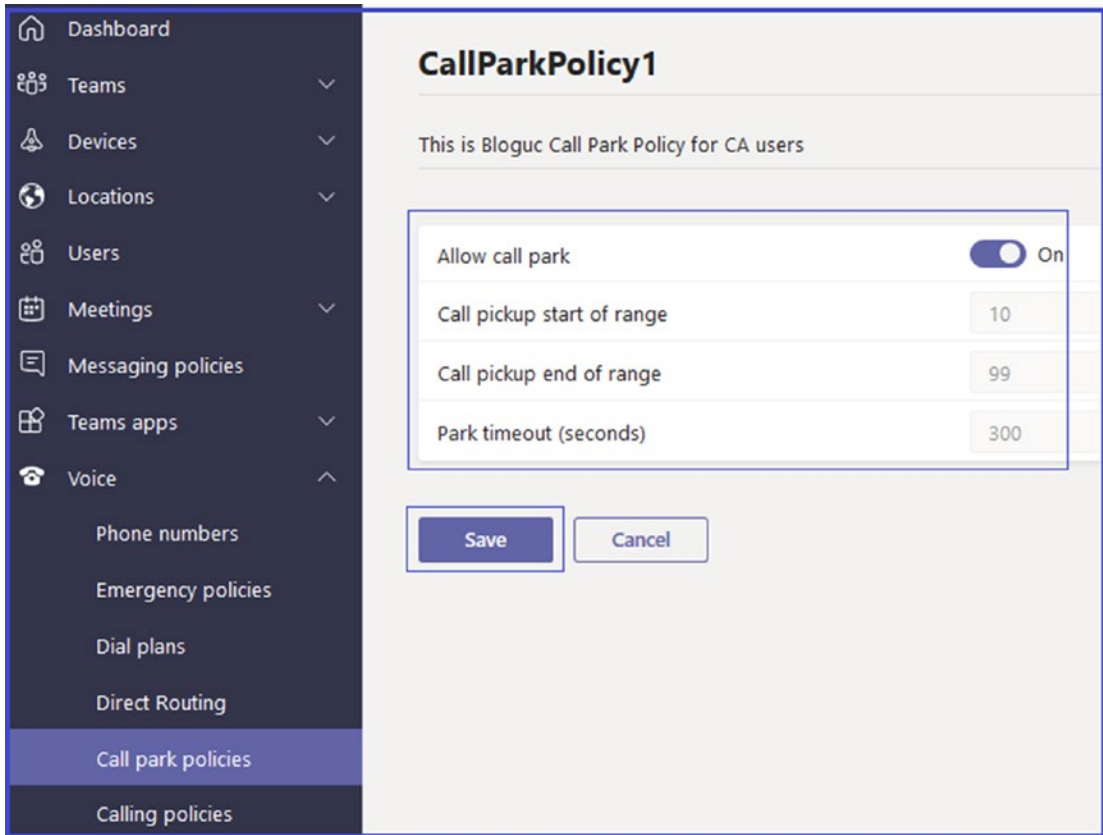


Figure 2-85. Call park policy

3. Click Save to commit the changes.

Assigning a Call Park Policy to a User

To assign a call park policy to one or more users, follow these steps.

1. Log in to Teams admin center and then navigate to Voice. Select Call Park Policies.
2. Select the policy by clicking to the left of the policy name and then select Manage Users.
3. On the Manage Users page, 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. The example in Figure 2-86 shows that the policy is assigned to user Balu Ilag.

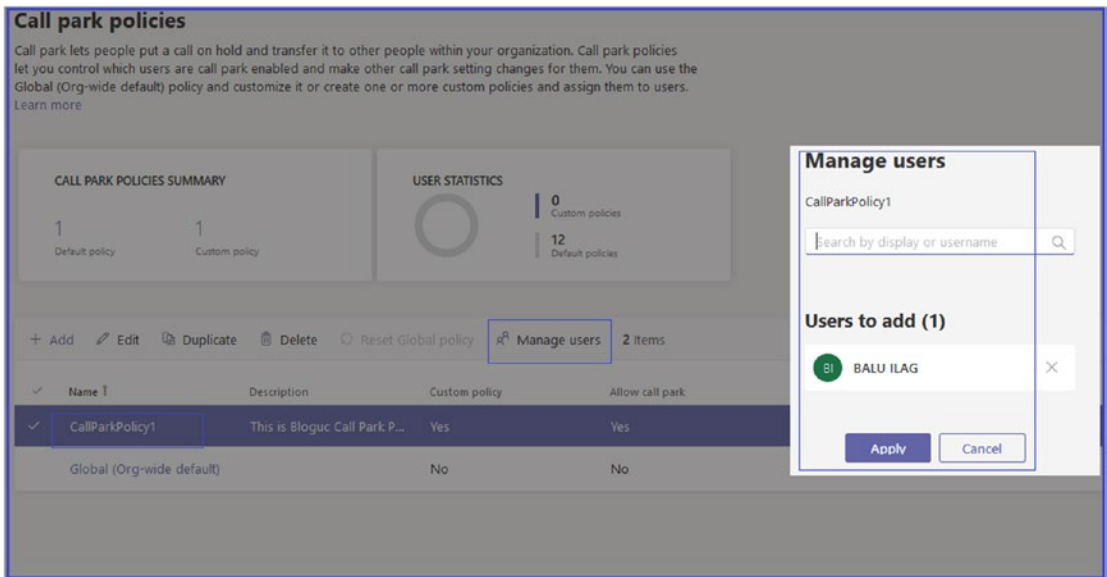


Figure 2-86. Assigning a call park policy

4. Once you finish adding users, click Save to commit the changes.

Managing Call Park Policy Using Windows PowerShell

To create a call park policy using PowerShell, use the PowerShell command `New-CsTeamsCallParkPolicy`.

```
Example: New-CsTeamsCallParkPolicy -Identity "CallParkPolicy1"  
-AllowCallPark $false
```

To grant the call park policy, use the `Grant-CsTeamsCallParkPolicy` PowerShell command.

```
Example: Grant-CsTeamsCallParkPolicy -PolicyName CallParkPolicy1  
-Identity "Balu Ilag"
```

To modify the default setting of a call park policy, use the `Set-CsTeamsCallParkPolicy` command.

```
Example: Set-CsTeamsCallParkPolicy -Identity Global -AllowCallPark $true
```

Calling Policy

Calling policies are used to control what calling features are available to users in Teams. As a Teams admin you can use the Global (Org-wide default) policy and customize it or create one or more custom calling policies for users who have phone numbers in your organization. In Teams, calling policies assist admins to determine which calling and call forwarding features will be available to your users. These policies determine whether a user can make private calls, use call forwarding or simultaneous ringing to other users or external phone numbers, route calls to voicemail, send calls to call groups, use delegation for inbound and outbound calls, and many more options.

Creating a Custom Calling Policy

To create a custom calling policy, follow these steps.

1. Log in to Teams admin center and navigate to Voice. Select Calling Policy and then click + Add.
2. On the Calling Policy page, shown in Figure 2-87 turn on the features that you want available in your calling policy (note that all features are turned off by default).

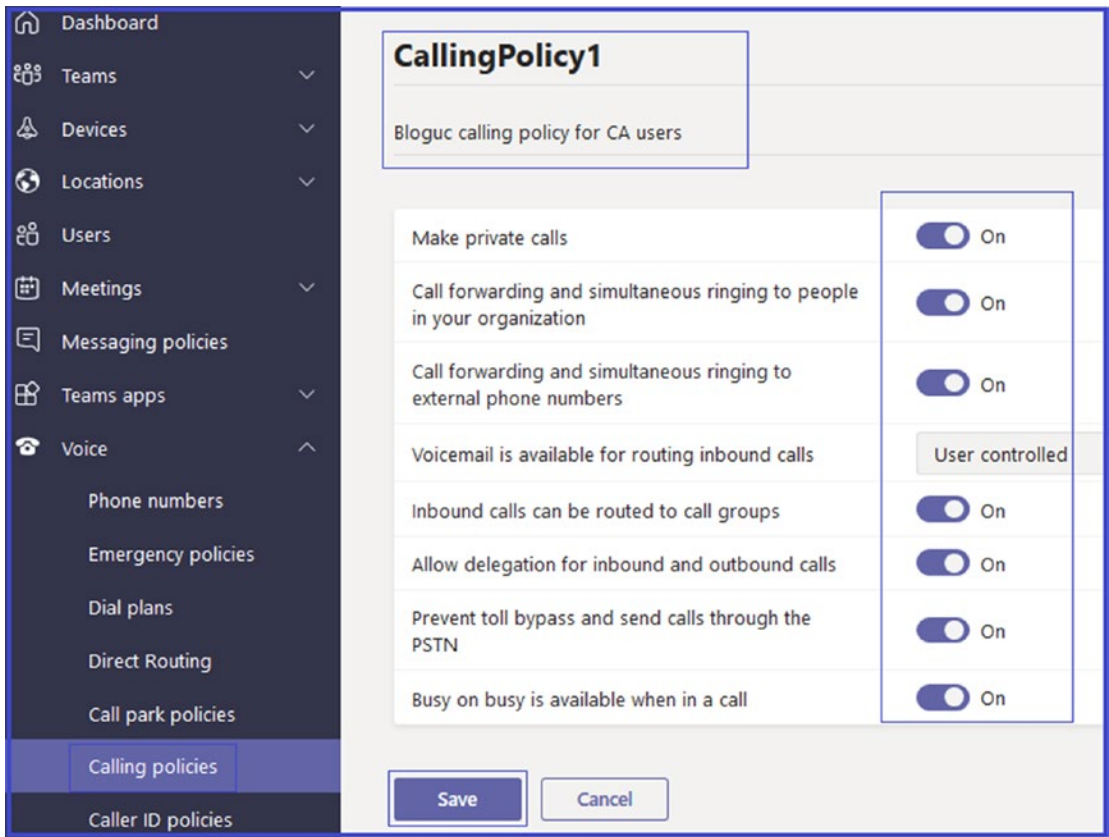


Figure 2-87. *Creating a calling policy*

For example, to control whether users can route inbound calls to voicemail, for the Voicemail Is Available For Routing Inbound Calls feature, select Always Enabled or User Controlled. To prevent routing to voicemail, select Always Disabled.

3. Once all features are set up, click Save to commit the changes.

Assigning the Calling Policy to a User

To assign a calling policy to a user, follow this procedure.

1. Log in to Teams admin center and navigate to Voice. Select Calling Policy and then select the policy name. Click Manage Users.
2. On the Manage Users page, shown in Figure 2-88, search for the user's name, select the user's name, and then click Add.

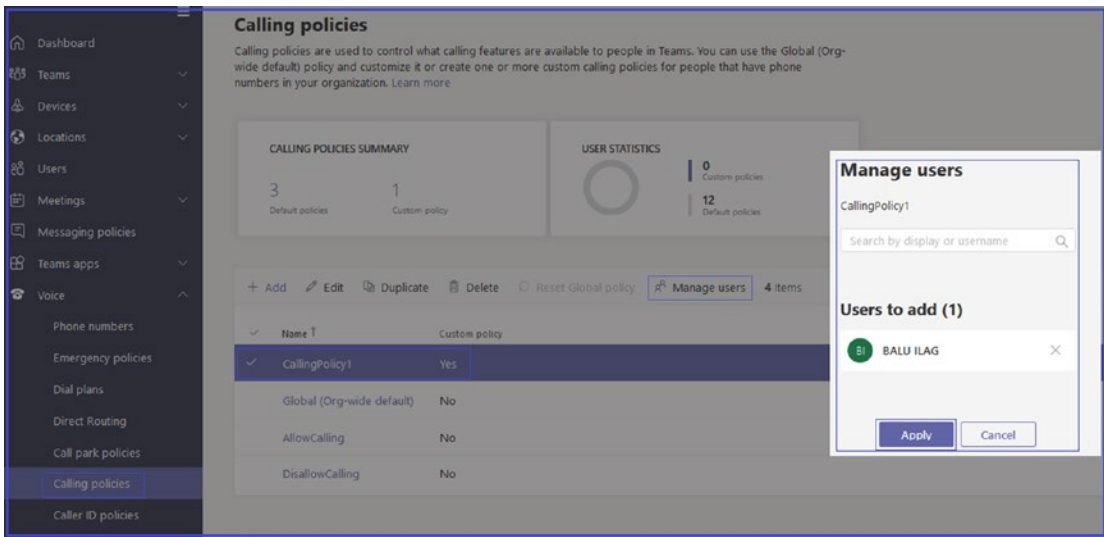


Figure 2-88. Assigning a calling policy to a user

3. Click Apply.

Calling Policy Settings

As an admin, you must know what different settings a Teams calling policy has. For reference, here are brief details for each setting.

- *User Can Make Private Calls:* This option controls all calling capabilities in Teams, so if you want to turn off all calling functionality in Teams, this option should be turned off.
- *Call Forwarding And Simultaneous Ringing To Other Users:* This option allows incoming calls to be forwarded to other users or to ring another person at the same time.
- *Call Forwarding And Simultaneous Ringing To External Phone Numbers:* This option allows incoming calls to be forwarded to an external number (or to ring an external number at the same time).
- *Make Voicemail Available For Routing Inbound Calls To Users:* This option allows inbound calls to be sent to voicemail. There are three options within this setting: Always Enabled, Always Disabled, and User Controlled (the user decides if he or she wants this option to be active).

- *Inbound Calls Routing To Calls Groups*: This option allows incoming calls to be forwarded to a call group.
- *Allow Delegation For Inbound And Outbound Calls*: This option allows inbound calls to be routed to delegates, who can then make outbound calls on behalf of the users (for whom they have delegated permissions).
- *Prevent Toll Bypass And Send Calls Through The PSTN*: This option allows calls to be sent through the PSTN and incur charges (rather than sending them through the network and bypassing the tolls).
- *Busy On Busy Is Available While In A Call*: This option, which is used in Teams calling policies, determines how incoming calls are handled when the intended user is already in a call. For example, you can set this option to reject the incoming call with a busy signal. This option is disabled by default, but it can be enabled at the tenant level or at the user level [82].

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, his or her 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 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 [2-89](#) shows these Caller ID settings.

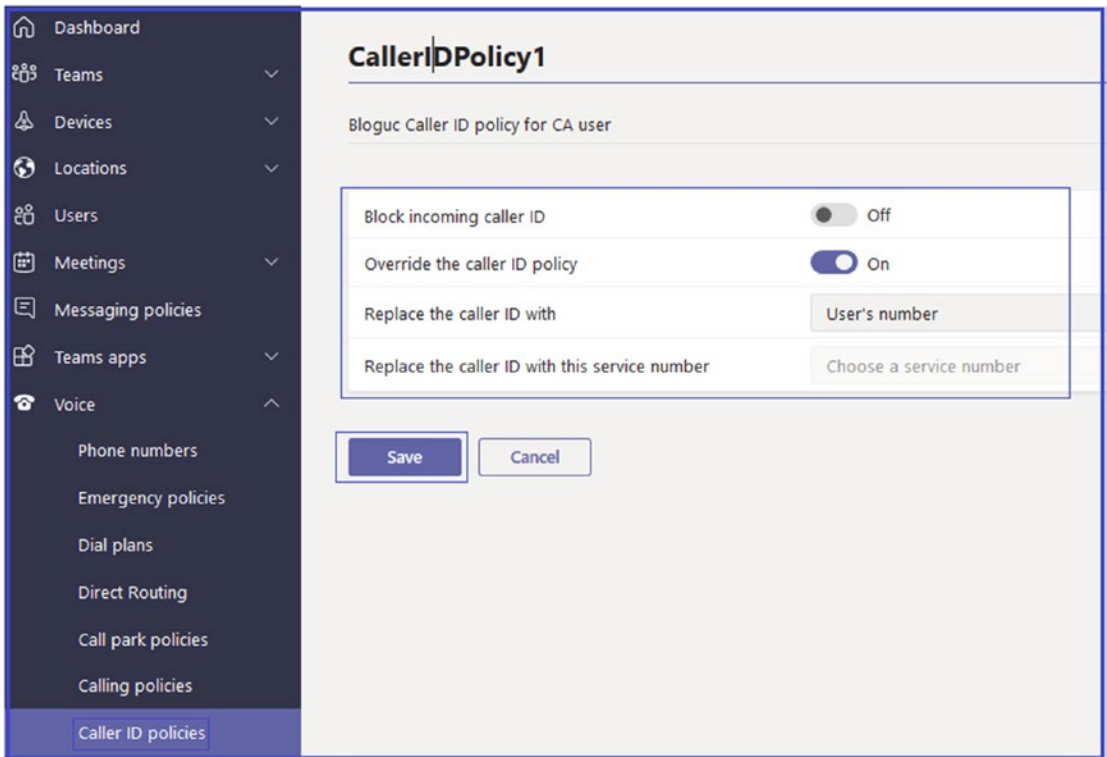


Figure 2-89. Caller ID policy

3. Once you are done configuring the caller ID settings, click Save.

Assigning a Custom Caller ID Policy to Users Through PowerShell

Once you create a custom caller ID policy, the next step is to assign it to users by using the Skype for Business Online PowerShell module. The following commands provide examples of using PowerShell to update custom caller ID policies. You should run the following command to assign the custom policy Support Caller ID Policy to bilag@bloguc.com. Remember, you cannot assign a caller ID policy to a user using Teams admin center.

```
Grant-CsCallingLineIdentity -Identity bilag@bloguc.com -PolicyName
"CallerIDPolicy1"
```

You should run the following commands to assign a custom policy to multiple users of a group using the Azure AD PowerShell module and looping through all members of a group:

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

Then get the members of the specified group:

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

Next, assign all users of the group a custom caller ID policy, such as CallerIDPolicy1:

```
$members | ForEach-Object {Grant-CsCallingLineIdentity -PolicyName  
"CallerIDPolicy1" -Identity $_.EmailAddress}
```

Policy Packages

Policy assignment is another important area that the Teams administrator has to work on. Microsoft made policy assignment a bit easier by providing policy packages. Policy packages allow Teams admins to control Teams features that they want to allow or restrict for specific sets of users across the organization.

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 an organization. The definitions in these policy packages aren't meant to assist with regulatory compliance; rather, they are provided for your convenience and can be customized based on your own regulatory requirements. Each policy package in Teams is designed around a user role and includes predefined policies and policy settings that support the collaboration and communication activities that are typical for that role. Figure 2-90 shows some example policy packages.

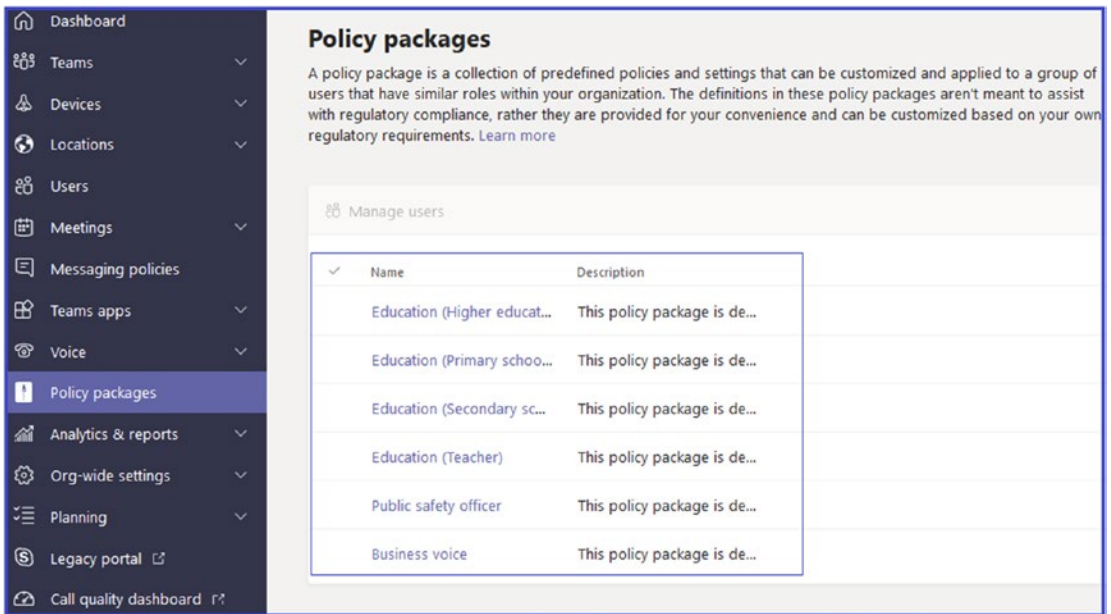


Figure 2-90. Policy packages

As an admin, you can assign policies to groups of users using PowerShell. When you want to assign a policy to a group, first you have to use PowerShell to pipe it to a group and then members, and then you could assign the policy. However, Microsoft is reducing this three-step process to one step, so you will be able to assign a policy to a user with a single PowerShell command. This capability should be available soon. The following is the sample command.

```
New-CsGroupPolicyAssignment -GroupId HR@bloguc.com -PolicyType
TeamsMeetingPolicy -PolicyName BlogucMeetingPolicy1 -Priority 1
Get-CsGroupPolicyAssignment -PolicyType TeamsMeetingPolicy
```

Policy assignment to security groups through PowerShell is not available as this writing, but Microsoft will be adding the functionality for assigning a policy to a security group in the future.

Analytics & Reports

Teams reporting is very 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 Teams admin center.

The Analytics & Reports tab in 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 though 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 [83].

Reports Available in Teams Admin Center Under Teams 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 2-91.

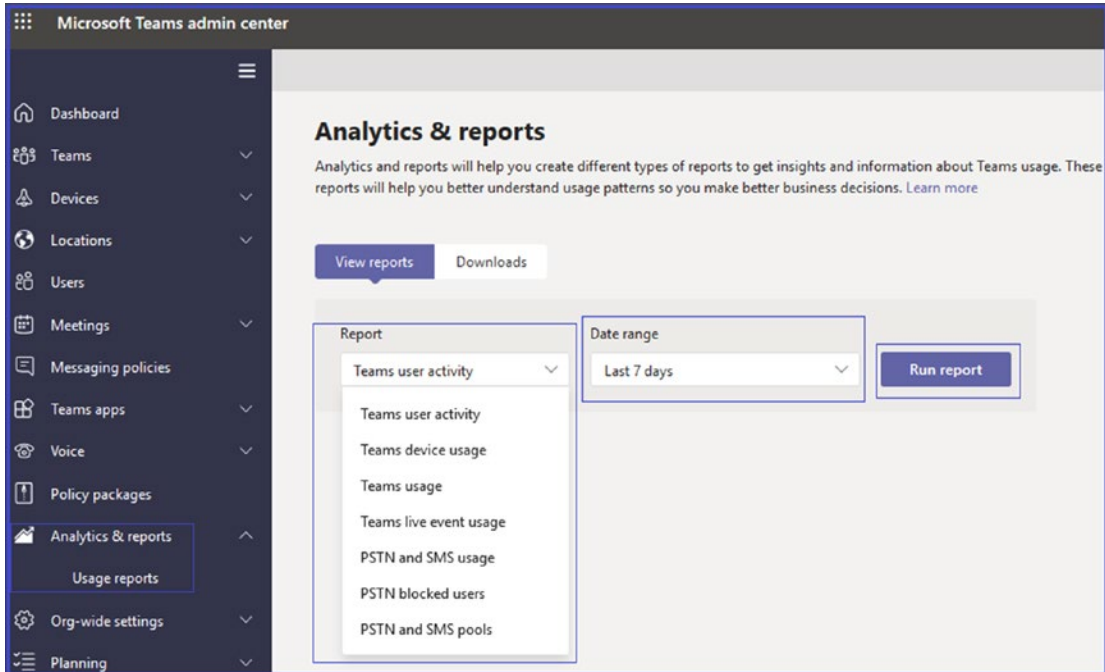


Figure 2-91. Available reports in Teams admin center

- *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.
- *Teams Device Usage*: This report gives information on whether users are using Windows, Mac, iOS, or Android devices to access the Teams app.
- *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 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.
- *PSTN And SMS Usage*: This report offers usage information on Calling Plans as well as Direct Routing.
 - *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.
- *PSTN Blocked Users*: This report offers details of display name, phone number, reason, the type of action, and the date and time of the action.

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: 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.

Teams Usage Reports

To access the Teams usage report, follow these steps.

1. Log in to Teams admin center, then navigate to Analytics & Reports. Select Usage Reports.
2. On the Usage Reports page, click the View Reports tab. From the Report drop-down list, select Teams Usage.
3. From the Date Range drop-down list, select the duration (current Teams usage reports are available only for 7 and 28 days).
Once you select the date range, click Run report. Figure 2-91 shows the Teams usage report for the last seven days for Bloguc Organization.

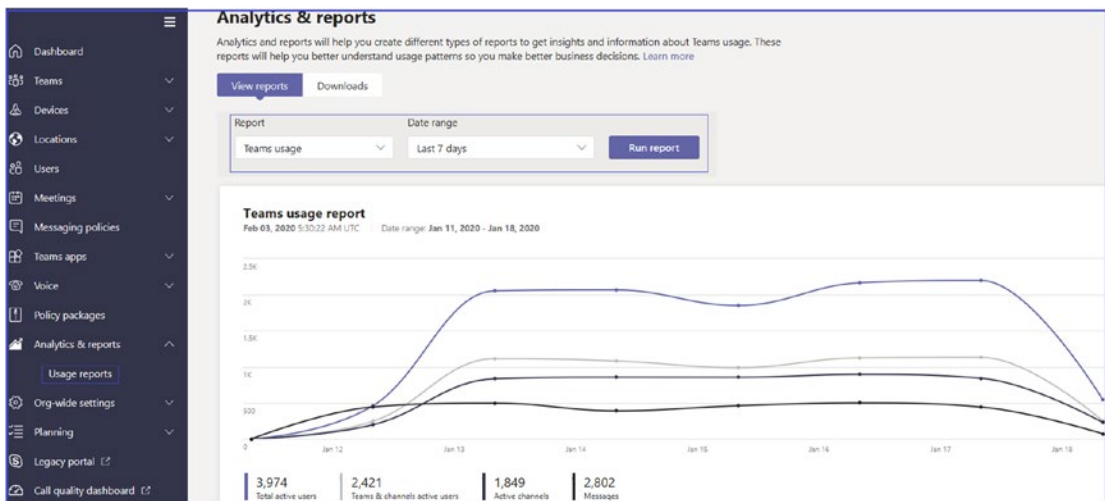


Figure 2-92. Teams usage report

The Teams usage activity report can be seen for the trends in the last 7 or 28 days. As an admin, you can filter what you see on the chart by clicking an item. For example, in Figure 2-92, when you click Total active users, Teams & channels active users, Active channels, or Messages, you will see only the information related to that metric. For example, Figure 2-93 shows only the Teams & channels active users information.



Figure 2-93. Teams and channel active users

Another important thing that Teams reports provides is an export option. An admin can export the report to a .csv file for offline analysis. To export the report, you can simply click Export To Excel. On the Downloads tab (see Figure 2-94), click Download to download the report when it is prepared.

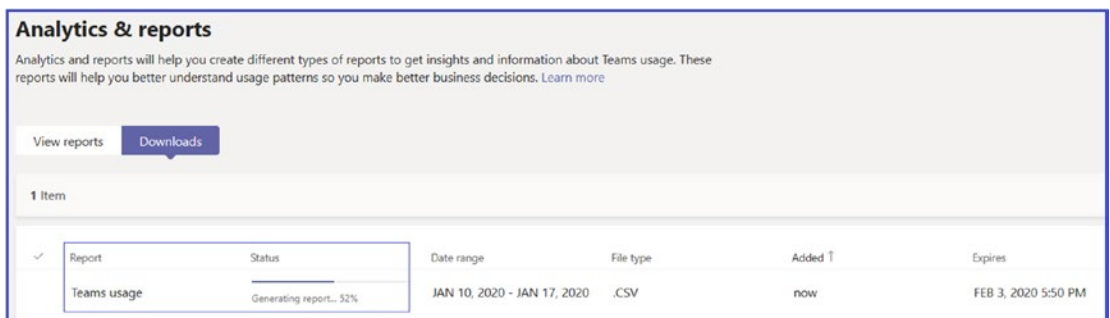


Figure 2-94. Exporting a report

Teams Reports Allow Customization Using Table Columns

Teams reports provide some customization by allowing table columns selection. As per your requirements, you can enable or disable table columns. This is easily achieved by clicking the Settings (gear icon) button. Figure 2-95 shows an available columns list for customizing a table.

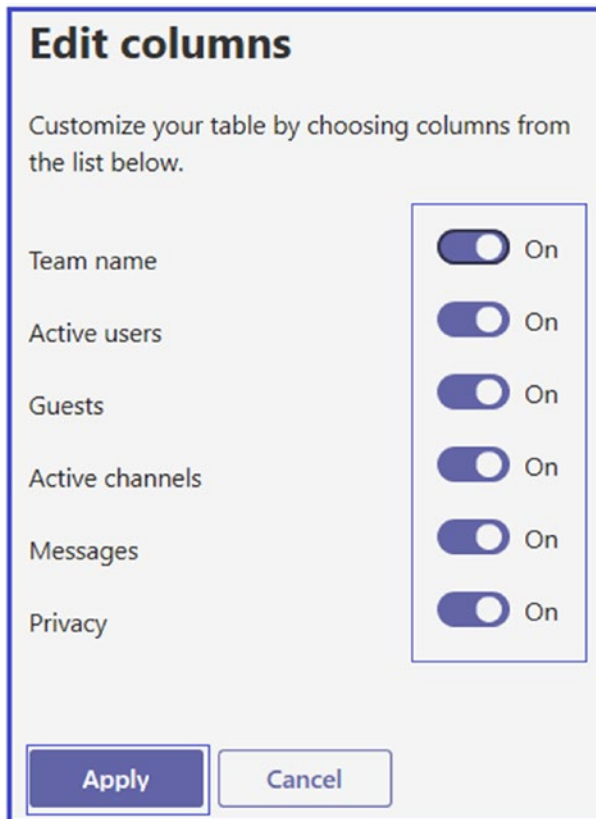


Figure 2-95. Customizing Teams report columns

Note Active users is a measure of the number of unique users who perform an action in Teams during the specified date range.

Active channels measures the number of channels of a team in which users perform an action during the specified date range.

Teams User Activity Report

The Teams user activity report is another popular and useful report. It gives a comprehensive view of which types of activities the users within the organization are performing in Teams. For example, you as an admin can see how many users communicate through one-to-one calls and chat, how many users communicate through channel messages, and how many users are involved in private chat messages. To access the Teams user activity report, follow these steps.

1. Log in to Teams admin center and navigate to Analytics & Reports. Select Usage reports. On the View Reports tab, from the Report drop-down list, select Teams User Activity. Next, from the Date Range drop-down list, select a period of either Last 7 Days or Last 28 Days and then click Run Report (see Figure 2-96).



Figure 2-96. Teams user activity report

Note Every report has a date for when it was generated. The reports usually reflect a 24- to 48-hour latency from time of activity.

2. You can filter what you see on the chart by clicking an item in the legend. For example, click 1:1 calls, Channel messages, or Chat messages to access only the information related to that metric. You can export the report to a .csv file for offline analysis. To do so, click Export to Excel, and then on the Downloads tab, click Download to download the report when it is available.

Teams Live Event Usage Reports

Teams live events are used for large events in one-to-many formats. A presenter shares audio and video and attendees see the video and hear the audio with limited interaction via Q&A. Because live events are very useful, so is this report. In live event usage reports, you can view usage information, including event status, start time, views, and production types for each event. This report is more useful for understanding usage trends and seeing who in your organization schedules, presents, and produces live events. To access the Teams live event report, perform this procedure, illustrated in Figure 2-97.

1. Log in to Teams admin center, and navigate to Analytics & Reports. Select Usage Reports. On the View Reports tab, from the Report drop-down list, select Teams Live Event Usage.
2. Select a predefined or custom date range. You can set a range to show data for up to a year, six months before and after the current date.
3. (Optional) In the Organizer drop-down list, you can select to show only live events organized by a specific user.
4. Click Run Report.

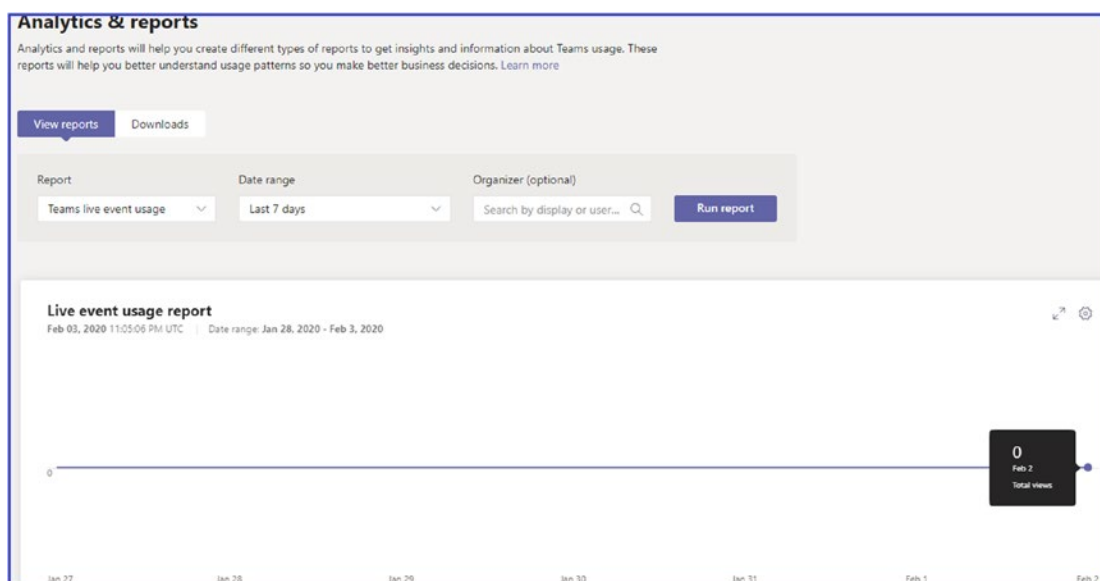


Figure 2-97. Teams live event report

The resulting table displays a breakdown of each live event (start time, organizer, producer, presenter, event status, and production type).

If you would like to see a summary of the details of a live event that lists all the files, including transcripts and recordings, associated with the event, you can do that on the Live Event Details page. If you would like to view or download the file, click the file name.

Teams Device Usage Reports

The Teams device usage report in the Microsoft Teams admin center provides information about how users connect to Teams. You can use this report to see the devices that are used across your organization, including how many use Teams from their mobile devices. To view the Teams device usage report, perform the following steps.

1. Log in to Teams admin center, navigate to Analytics & Reports. Select Usage Reports. On the View Reports tab, from the Report drop-down list, select Teams Device Usage.
2. Next select the date range, and then click Run Report. An example report is shown in Figure 2-98.

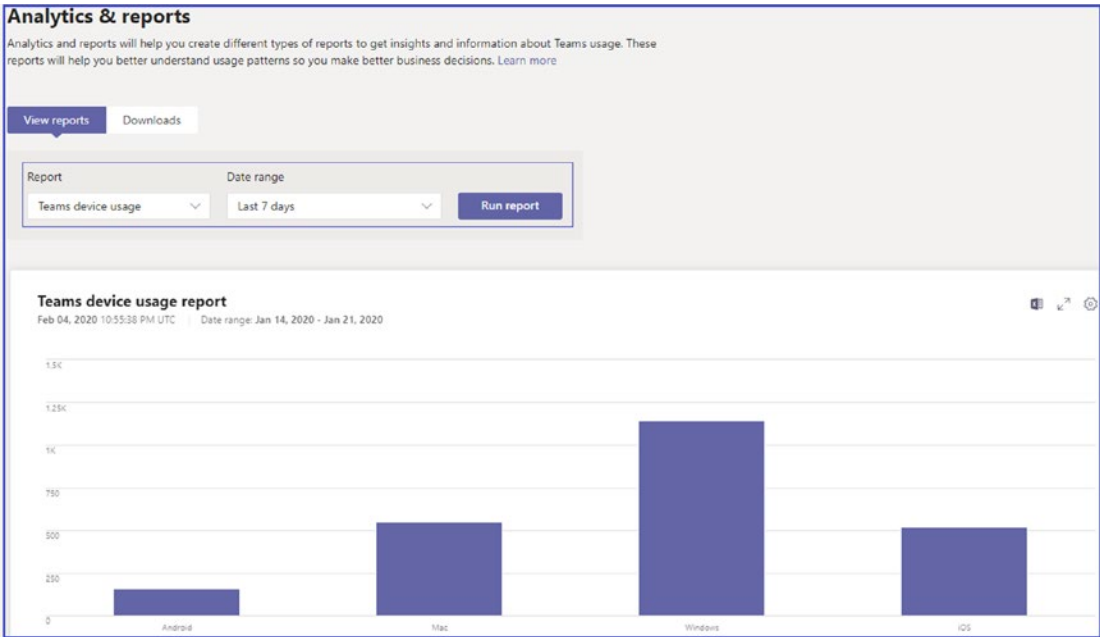


Figure 2-98. Teams device usage report

The resulting report gives you a breakdown of device usage by user (display name, what type of device was used [Windows, Mac, Android, iOS], period of last activity). You can export the report to a .csv file for offline analysis. Click Export to Excel, and then on the Downloads tab, click Download to download the report when it is ready.

Microsoft might add more analytics and reports in the future for per-team and usage scenarios.

Org-wide Settings

In Teams admin center, under Org-wide Settings, an admin can manage and configure org-wide settings such as external access, guest access, Teams settings, Teams upgrade, holidays, and resource accounts, as shown in Figure 2-99.

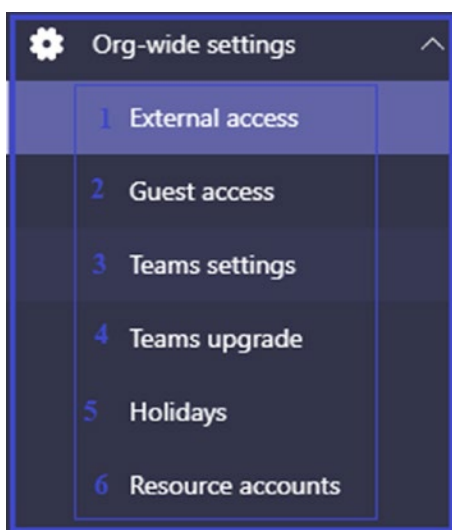


Figure 2-99. Teams org-wide settings

External Access

External access lets your Teams and Skype for Business users communicate with other users that are outside of your organization. By default, your organization can communicate with all external domains. If you add blocked domains, all other domains will be allowed but if you add allowed domains, all other domains will be blocked.

External access is a technique for external Teams users from a whole domain or tenant to find, call, chat, and set up meetings with your organization's teams. It will be beneficial for users in your organization to use Teams to contact users outside of your organization domain. Also, Teams users can find and contact other organizations via external access. If you remember federation access in the Skype for Business (Lync) world, then this is the same federation access in Teams world.

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 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 external to 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.

Enabling External Access in Teams

As mentioned earlier, external access enables your Teams users to reach out to external organization users for peer-to-peer communications. The Teams admin center provides a way for Teams admins or security admins to enable or disable external access for Teams.

1. To enable external access, log in to Teams admin center using the Teams service administrator role permission or global admin permission and navigate to Org-wide Settings.
2. Under Org-wide Settings, select External Access and turn on or off external access for your organization.
3. Once you turn **on** the option Users Can Communicate With Skype For Business And Teams Users, this switch will enable external communication with Skype for Business Online users and Teams users based on the domain allowed setting.

Enabling Skype For Business Users Can Communicate With Skype Users will enable Skype for Business Online users to communicate with consumer Skype users.

For example, Figure 2-100 shows external access enabled for Skype for Business Online and Teams, but not enabled for Skype consumer users. You as a Teams admin or security admin can make this decision based on your organization's requirements.



Figure 2-100. Allowing external (federation) access

Once you turn on the Users Can Communicate With Skype For Business And Teams Users option, the next thing you need to decide is how you want to control external access. For example, Bloguc Organization decides to allow specific domains and block all domains.

If you want to allow external access for all domains that are using Skype for Business Online and Teams, then turning on the Users Can Communicate With Skype For Business And Teams Users option under external access is enough, as shown in Figure 2-101.

However, if an organization wants to enable granular control by allowing specific domains for external access and blocking all other domains, Microsoft Teams does provide granular control through Teams admin center and Windows PowerShell. After you turn on external access you need to allow or block domains based on your organization's requirements. As an admin you can allow specific domains, then add domains one by one. For example, Figure 2-101 shows that microsoft.com is allowed and all other domains are blocked.

Allowing Specific Domains and Block All Other Domains Using Teams Admin Center

To allow a specific domain, follow these steps.

1. Log in to Teams admin center and navigate Org-wide Settings. Select External Access and then click Add A Domain. In the Add A Domain box, enter the domain name. Figure 2-101 shows the microsoft.com domain typed. Select the Allowed option and then click Done.

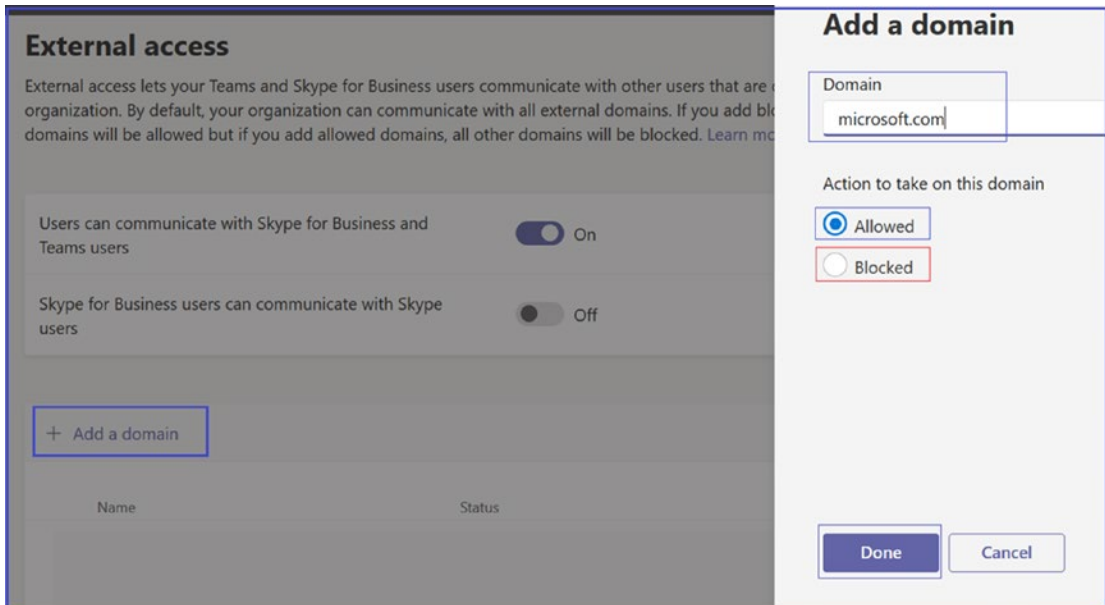


Figure 2-101. Allowing a specific external domain

As an example, Figure 2-102 shows the Bloguc Organization allowed the microsoft.com domain for external (federation) access in Teams, but blocked the abc.com domain for external access. Finally, click Save to commit the changes.

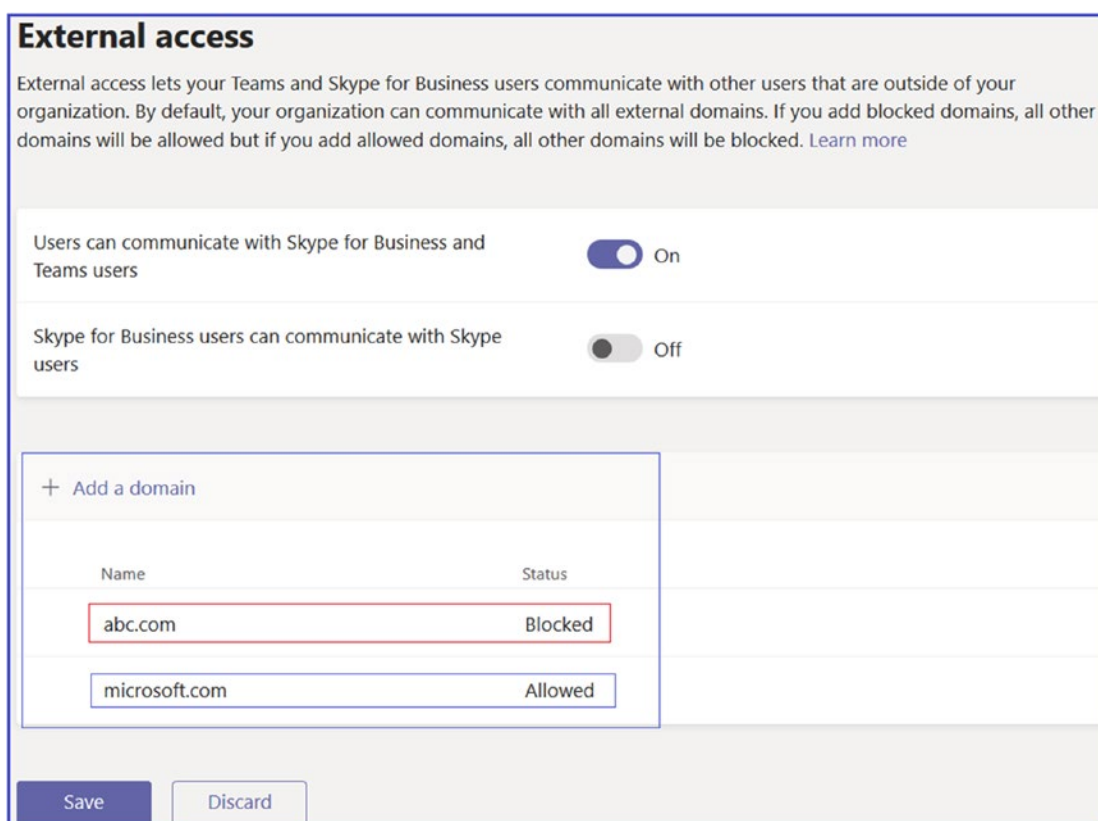


Figure 2-102. Allowing and blocking specific domains

Guest Access

Microsoft Teams offers external collaboration through two methods: guest access and external access, also known as federation access. We already learned about external access in previous topic, 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 Teams admin center and is turned off by default. To allow 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, first you as an admin 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 Bloguc Organization as a guest. The guest organization (Microsoft) will control the authentication layer and 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, he or she first needs to get invited through email or any other mechanism. Once the guest user accepts the invite, he or she gets 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, 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 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 level.
- *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 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.

Follow this procedure to enable guest access using Teams admin center:

1. To enable guest access in Teams, log in to Teams admin center and then navigate to Org-wide Settings.
2. Select Guest Access. Set the Allow Guest Access In Microsoft Teams option to On for your tenant organization, as shown in Figure 2-103.

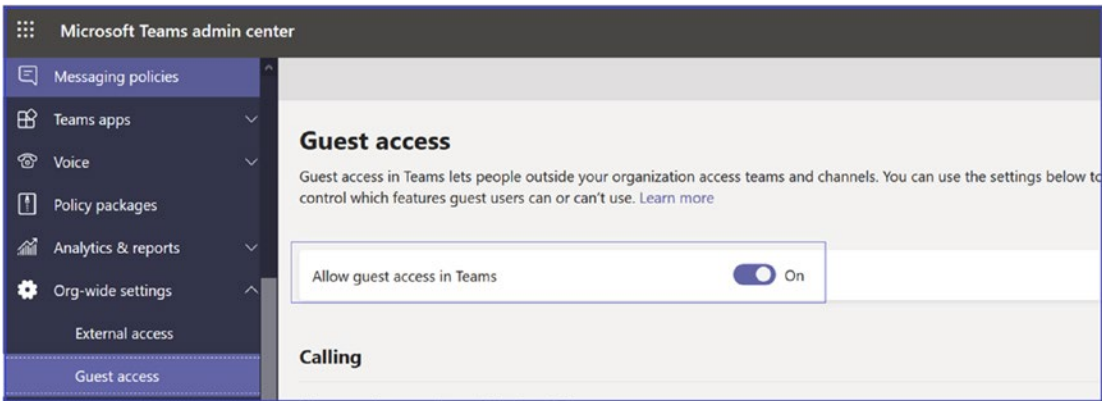


Figure 2-103. Enabling guest access

3. Under Calling and Meeting, and Messaging, set functionalities depending on the capabilities you want to allow for guest users.
 - *Make Private Calls:* Turn this setting on to allow guests to make peer-to-peer calls.
 - *Allow IP Video:* Turn this setting on to allow guests to use video in their calls and meetings.

- *Screen Sharing Mode*: This setting controls the availability of screen sharing for guest users.
 - Set this setting to Disabled to remove the ability of guests to share their screens in Teams.
 - Set this setting to Single Application to allow sharing of individual applications.
 - Set this setting to Entire Screen to allow complete screen sharing.
- *Allow Meet Now*: Turn this setting on to allow guests to use the Meet Now feature in Microsoft Teams. Figure 2-104 shows the available calling and meeting settings.

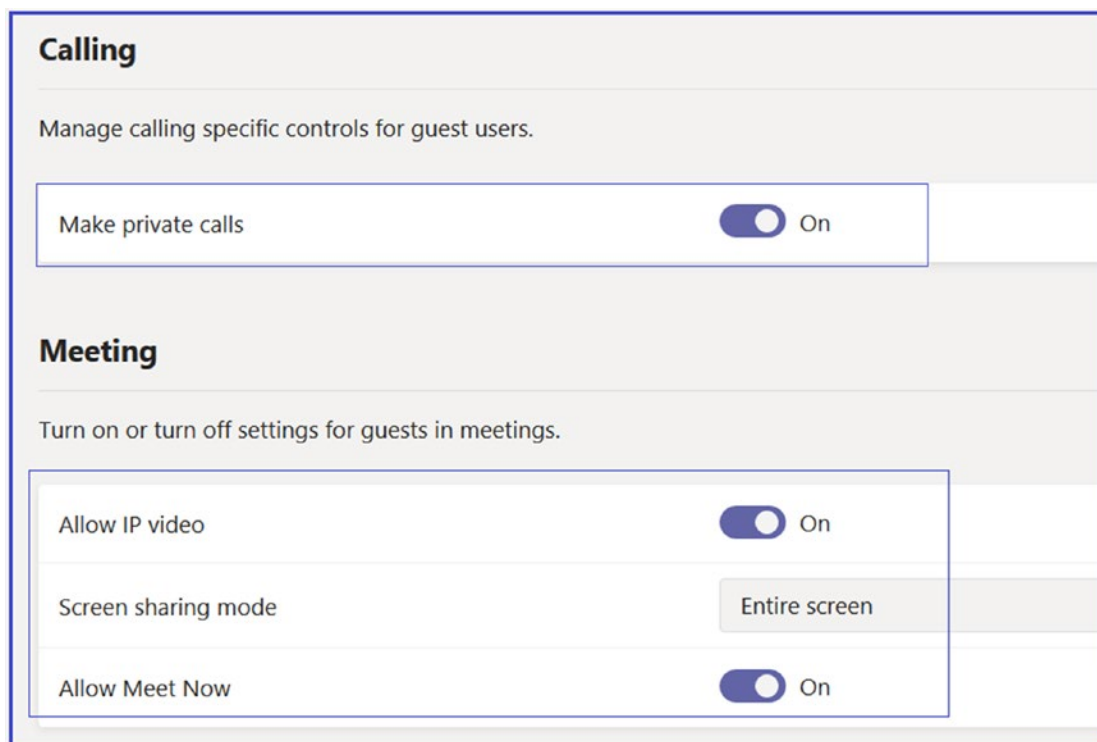


Figure 2-104. Guest access for calling and meetings

- *Edit Sent Messages*: Turn this setting on to allow guests to edit messages they previously sent.

- *Delete Sent Messages:* Turn this setting on to allow guests to delete messages they previously sent.
- *Chat:* Turn this setting on to give guests the ability to use chat in Teams.
- *Use Giphys In Conversations:* Turn this setting on to allow guests to use Giphys in conversations. Giphy is an online database and search engine that allows users to search for and share animated GIF files. Each Giphy is assigned a content rating.
- *Giphy Content Rating:* Select a rating from the drop-down list:
 - *Allow All Content:* Guests will be able to insert all Giphys in chats, regardless of the content rating.
 - *Moderate:* Guests will be able to insert Giphys in chats but will be moderately restricted from adult content.
 - *Strict:* Guests will be able to insert Giphys in chats but will be restricted from inserting adult content.
- *Use Memes In Conversations:* Turn this setting on to allow guests to use memes in conversations.
- *Use Stickers In Conversations:* Turn this setting on to allow guests to use stickers in conversations. Figure 2-105 displays all available messaging settings.

Messaging

Turn on or turn off settings for guests in chats or channel conversations.

Edit sent messages	<input checked="" type="checkbox"/> On
Delete sent messages	<input checked="" type="checkbox"/> On
Chat	<input checked="" type="checkbox"/> On
Use Giphys in conversations	<input checked="" type="checkbox"/> On
Giphy content rating	Allow all content
Use Memes in conversations	<input checked="" type="checkbox"/> On
Use Stickers in conversations	<input checked="" type="checkbox"/> On
Allow immersive reader for viewing messages	<input checked="" type="checkbox"/> On

Figure 2-105. Guest messaging settings

4. Once you set all options, click Save to commit the changes.

Note 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.

Teams Settings

Teams settings allow you 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

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. To enable notification and feeds, follow these steps.

1. Log in to Teams admin center and then navigate to Org-wide Settings. 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 2-106.
3. Once you have made the required changes, click Save to commit the changes.

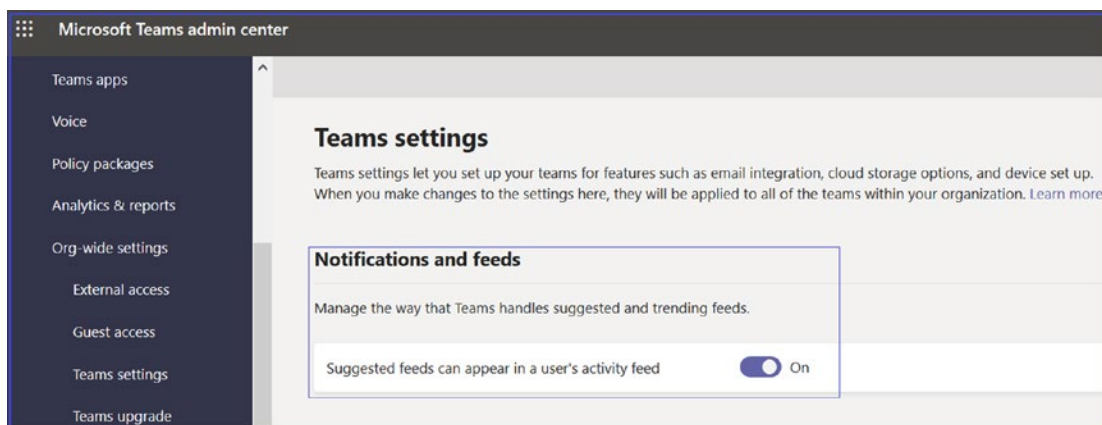


Figure 2-106. *Notifications and feeds*

Email Integration

Email integration is one of the most popular integration features among users. You as a Teams admin can use Teams admin center to configure email integration. This is very 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 very 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 very 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 selecting the More options (...) icon to the right of a channel’s name and then selecting Get Email Address (see Figure 2-107).

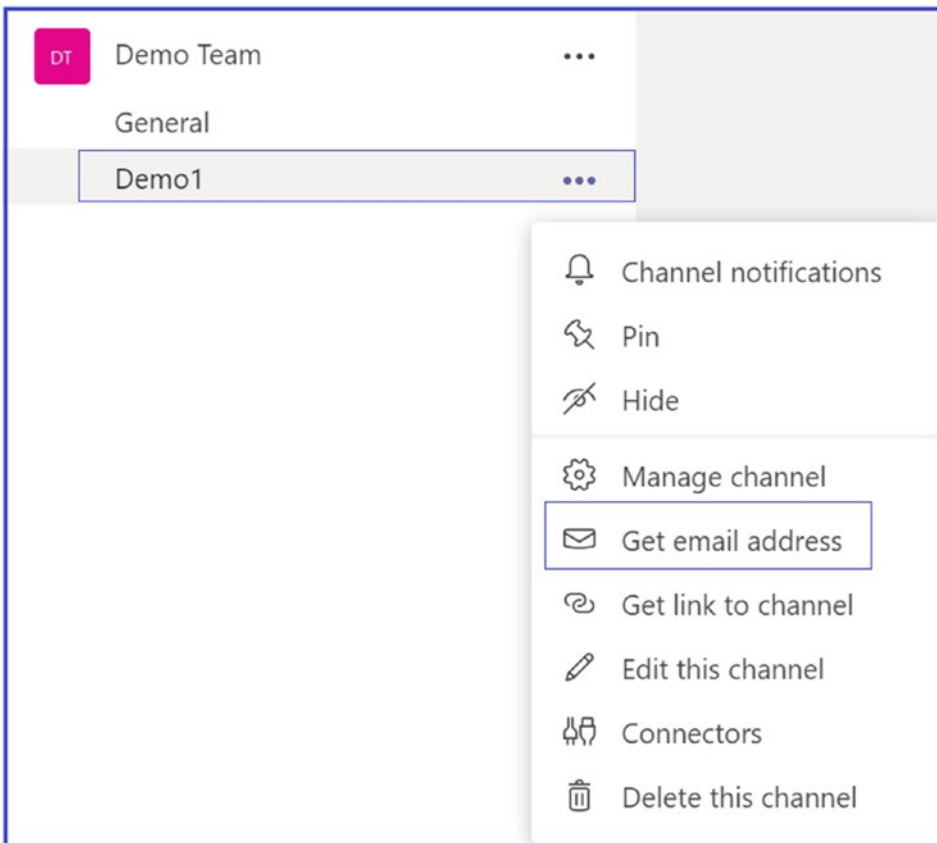


Figure 2-107. Retrieving the email address of a channel

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>. For example, demo channel email address, 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 Teams admin center and then navigate to Org-wide Settings. Select Teams Settings.
2. Under Email Integration, turn on the Allow Users To 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 2-108 shows the bloguc1.com and bloguc2.com SMTP domains added to accept the channel emails.

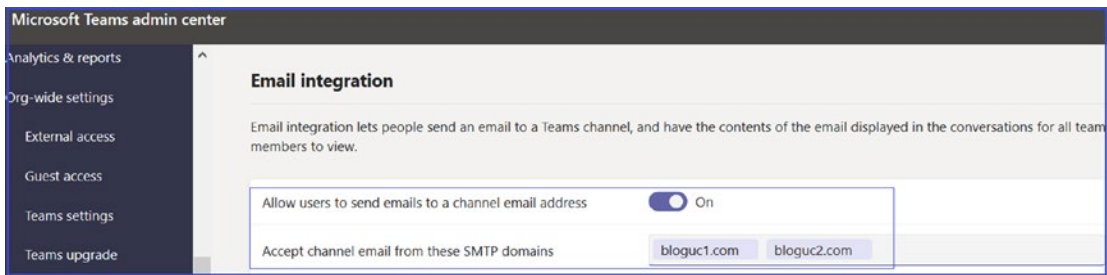


Figure 2-108. *Email integration*

Best Practices for Email Integration

Channel email addresses are lengthy and contain the Teams domain, which make them difficult to remember. It is 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.

- *Files:* You as an admin can turn on or turn off file sharing and cloud file storage options on the Files tab in Teams. Teams supports four types of file stores and a sharing option. The details of each option are as follows.
- *Citrix Files:* Files controls the availability of Citrix files as a third-party storage provider in Teams. As an admin, you want to restrict the use of third-party storage providers on the tenant level in Teams to all, some, or no other providers. This can be required if storage providers with storage locations outside of Europe are not allowed in your organization.

- *DropBox*: This controls the availability of DropBox as a third-party storage provider in Teams. As an admin you want to restrict the use of third-party storage providers on the tenant level in Teams to all, some, or no other providers. This can be required if storage providers with storage locations outside of Europe are not allowed in your organization.
- *Box*: This controls the availability of Box files as a third-party storage provider in Teams. As an admin you want to restrict the use of third-party storage providers on the tenant level in Teams to all, some, or no other providers. This can be required if storage providers with storage locations outside of Europe are not allowed in your organization.
- *Google Drive*: This controls the availability of Google Drive as a third-party storage provider in Teams. As an admin you want to restrict the use of third-party storage providers on the tenant level in Teams to all, some, or no other providers. This can be required if storage providers with storage locations outside of Europe are not allowed in your organization.

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 Teams admin center and then navigate to Org-wide Settings. Select Teams Settings.
2. Under Files, turn on or off the options for Citrix files, DropBox, Box, and Google Drive.
3. Once you have made the required changes, click Save to commit the changes. As an example, Figure 2-109 shows that Bloguc Organization allows all four types of file storage.

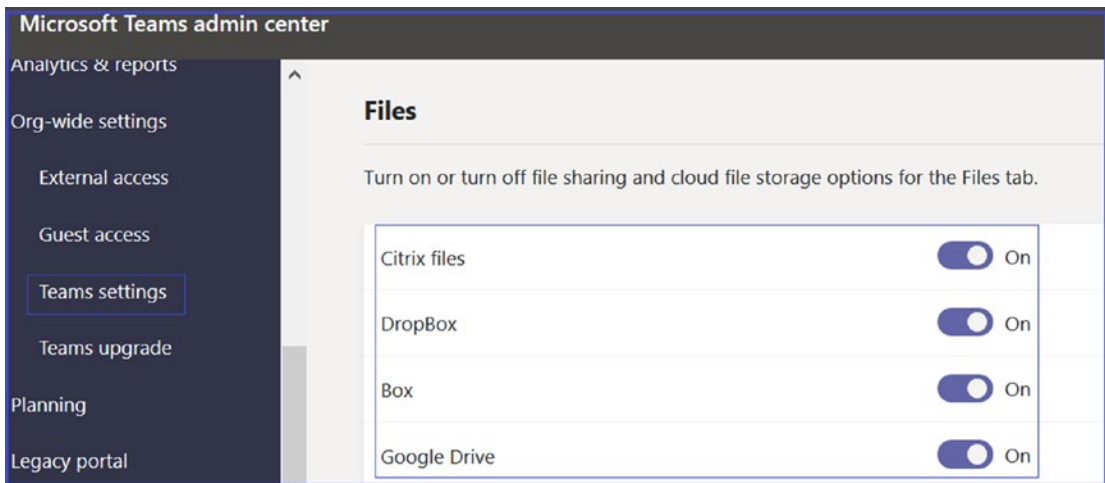


Figure 2-109. Teams settings for files

Organization

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 Teams admin center and then navigate to Org-wide Settings. 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 2-110 shows that Bloguc Organization allows the Organization tab to be displayed in chat.

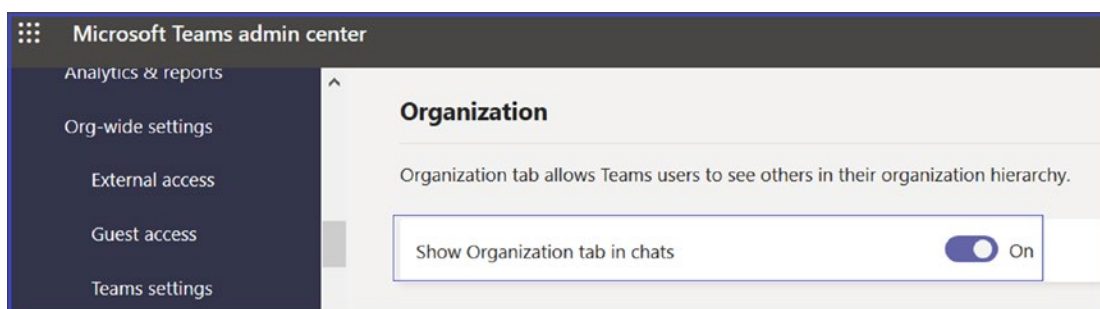


Figure 2-110. Teams settings organization

Devices

Teams provides organization-wide devices 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 to 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 Teams admin center and then navigate to Org-wide Settings. 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 2-111 shows the Bloguc Organization devices settings.

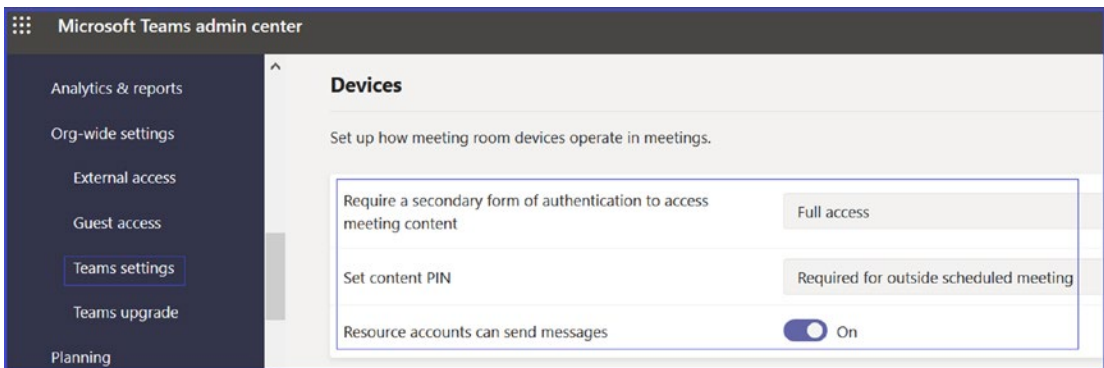


Figure 2-111. Teams settings for devices

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 to the 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 only work 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 scope directory search using an Exchange address book policy in your tenant, follow these steps.

1. Log in to Teams admin center and then navigate to Org-wide settings. 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 2-112 shows that the Bloguc Organization has enabled the scope directory search using an Exchange address book.

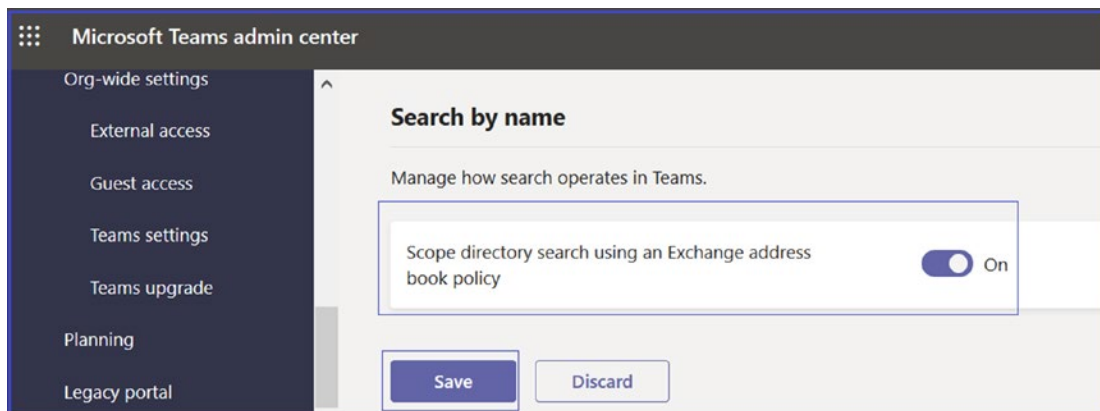


Figure 2-112. Teams setting a directory search by name

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.

Teams Upgrade

The Microsoft Teams 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 2-113 shows a default view of the Teams upgrade settings.

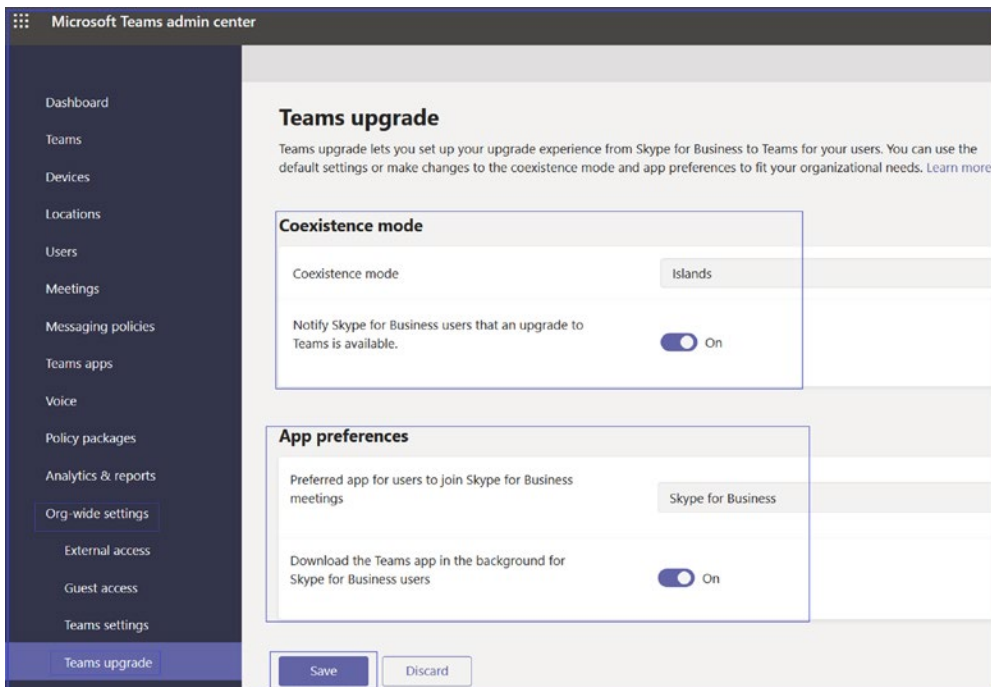


Figure 2-113. Teams upgrade settings

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

1. *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.
2. *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.
3. *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.
4. *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.

5. *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 [43].

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 2-114 shows details for all five upgrade modes.

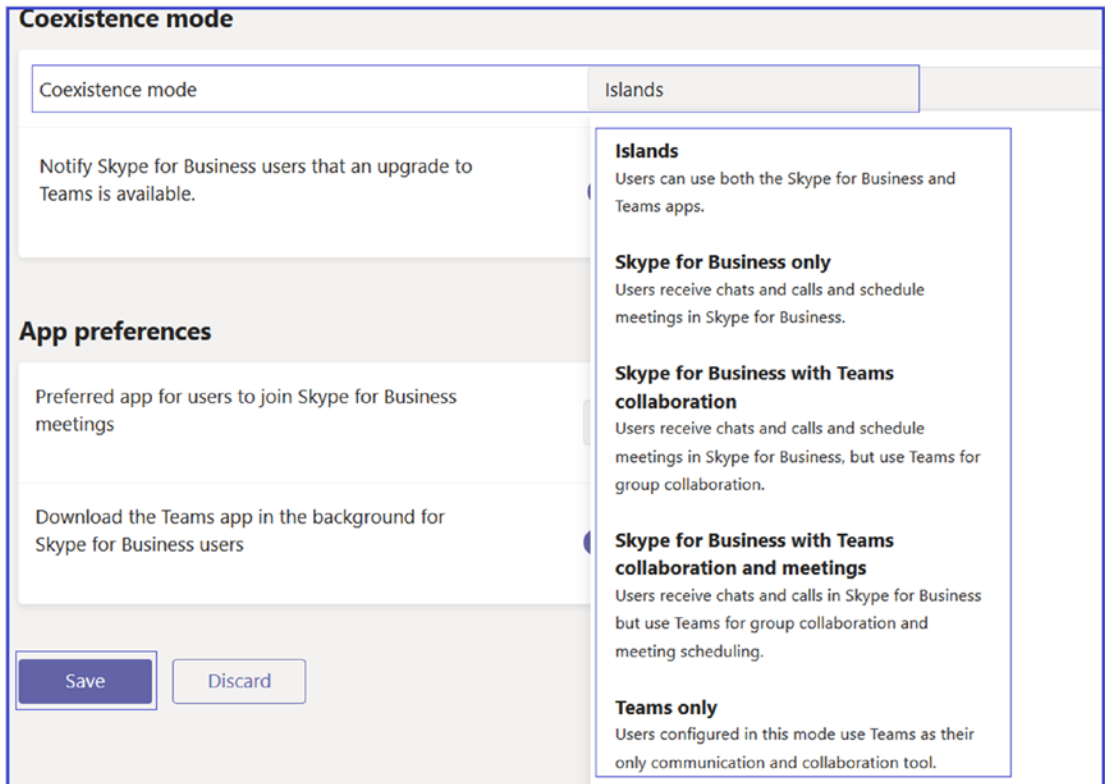


Figure 2-114. Teams coexistence modes

Setting Teams Upgrade Mode

Before enabling Teams upgrade mode for users, you as an admin must undertake extensive planning and preparation, including readiness of network infrastructure to allow Teams media traffic, setup of your firewall to allow Teams traffic seamlessly, 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 Org-wide Settings. Select Teams Upgrade.
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 would 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. Figure 2-115 shows all options enabled for the demo tenant.

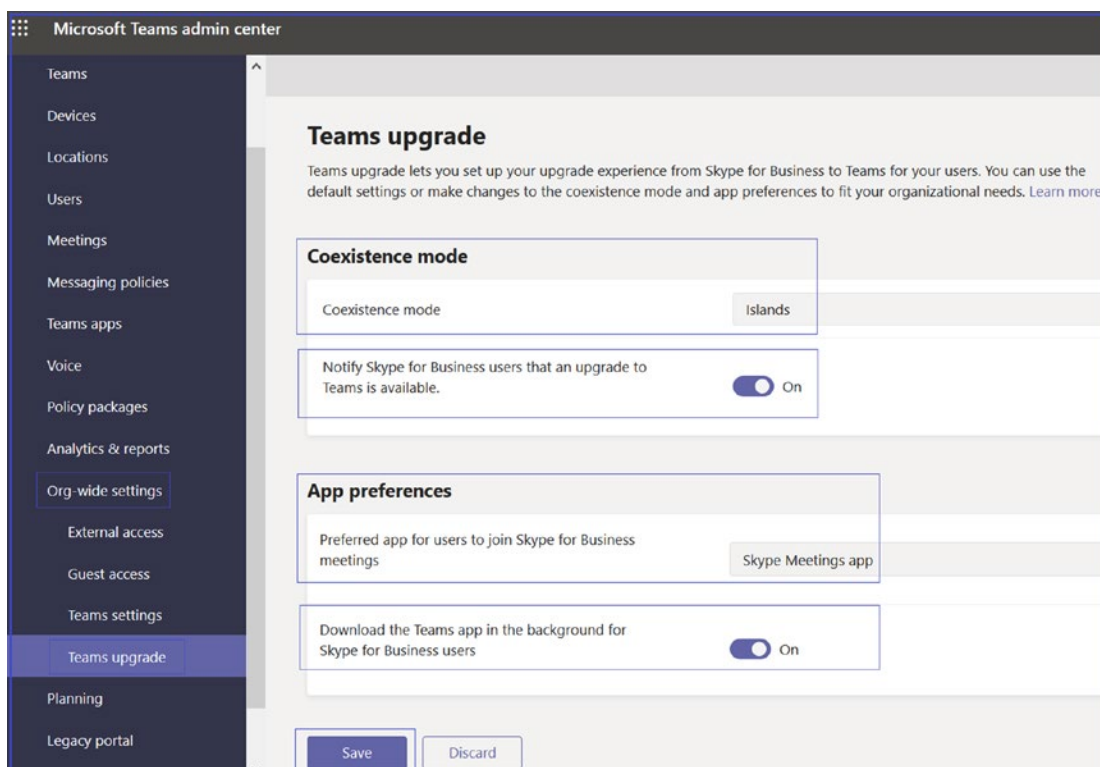


Figure 2-115. Teams upgrade options

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 Teams Admin Center

You learned 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 Teams admin center. To set a coexistence mode for an individual user, follow these steps.

1. Log in to 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 2-116 shows Teams Only assigned to user Chanda Ilag.

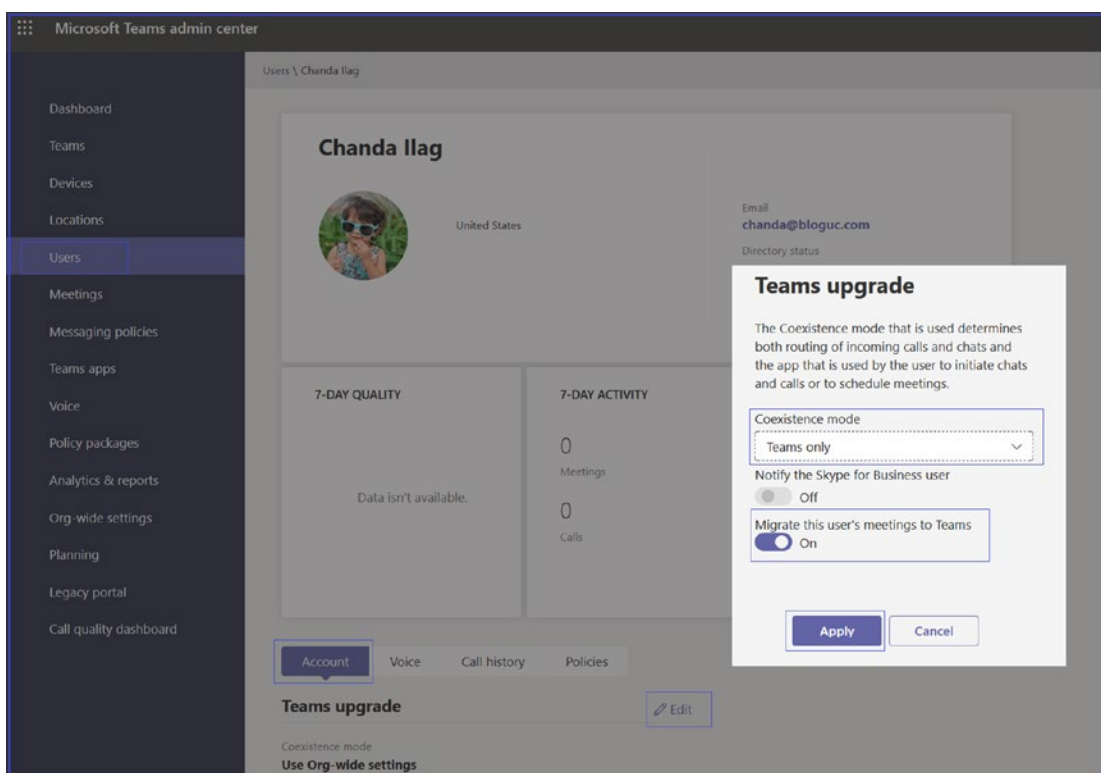


Figure 2-116. Assign a Teams upgrade mode

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 either 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
```

Planning

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 topic you will study how to use Teams Advisor and plan for Teams deployment. When planning the implementation of Microsoft Teams within your network, you must ensure that there is sufficient bandwidth, accessibility to all required IP addresses, correct configuration of ports, satisfied performance requirements for real-time media.

Advisor for Teams

Microsoft Teams has a new onboarding tool that helps you with Teams deployment in your organization, called Advisor for Teams. This tool was previewed earlier and now it is available to use. Advisor for Teams is a new tool that helps to bring your project team together and it allows you to plan a successful Teams deployment for your organization. Advisor for Teams provides recommended plans and a collaboration space for the deployment team to streamline the rollout of all the Teams workloads, including messaging, meetings, and calling workloads.

What Advisor for Teams Can Do

There are multiple things that Advisor for Teams can provide, and here we cover a few of the 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 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. Figure 2-117 shows Chat, teams, channels and apps selected. Click Create.

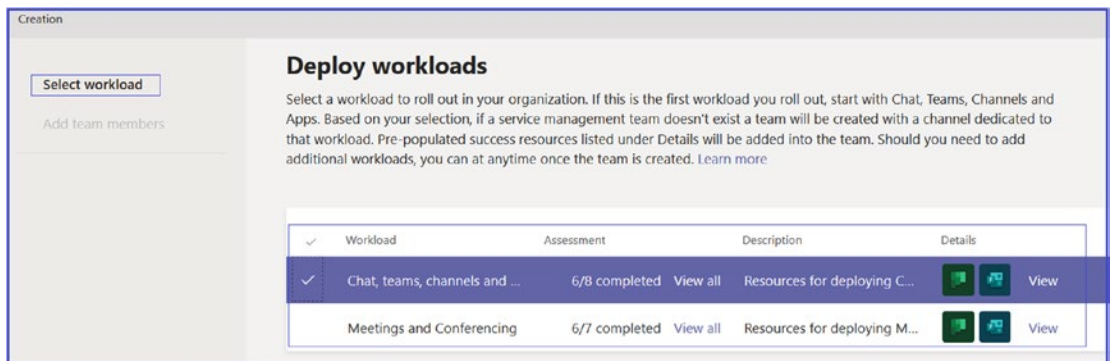


Figure 2-117. Deploying workloads

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 2-118.

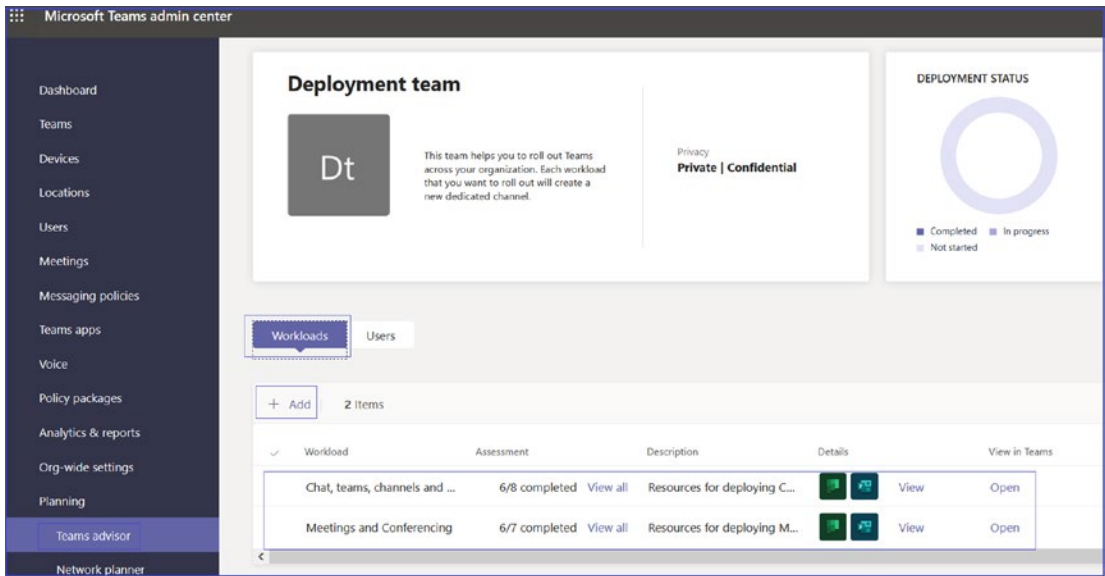


Figure 2-118. Two workloads are shown

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 2-119 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.

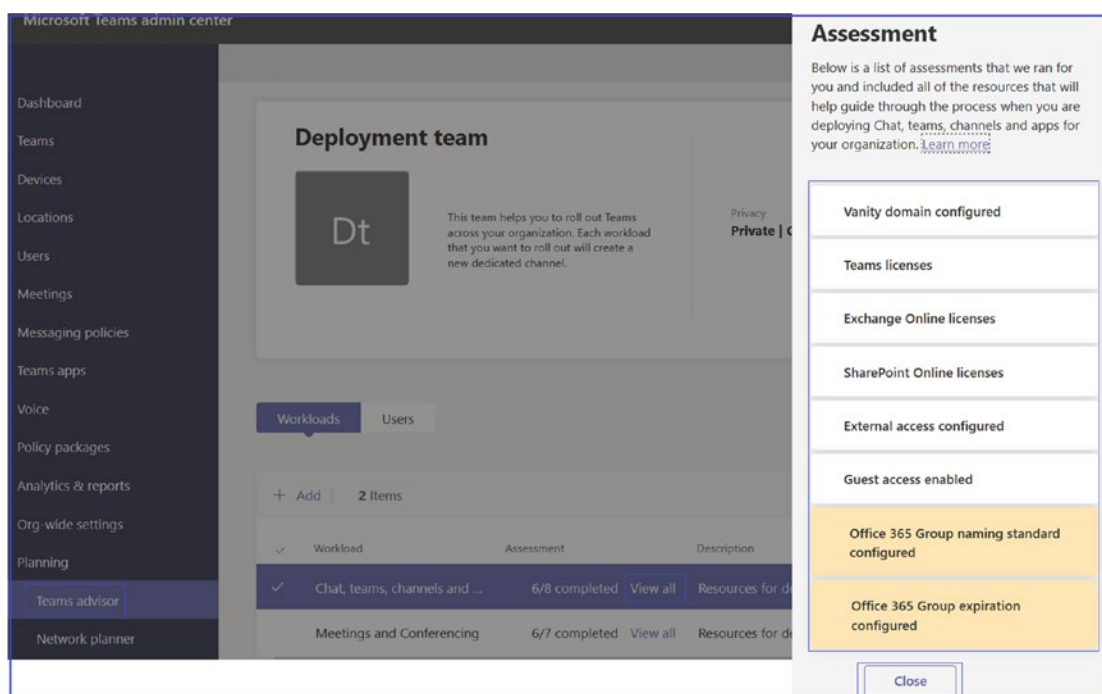


Figure 2-119. Advisor for Teams assessment

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 on 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 very easy; you can open the deployment team in Teams and add multiple members who are going to execute tasks.

Network Planner

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 planner tool through Microsoft Teams admin center. Select Planning and then Network Planner, as shown in Figure 2-120.

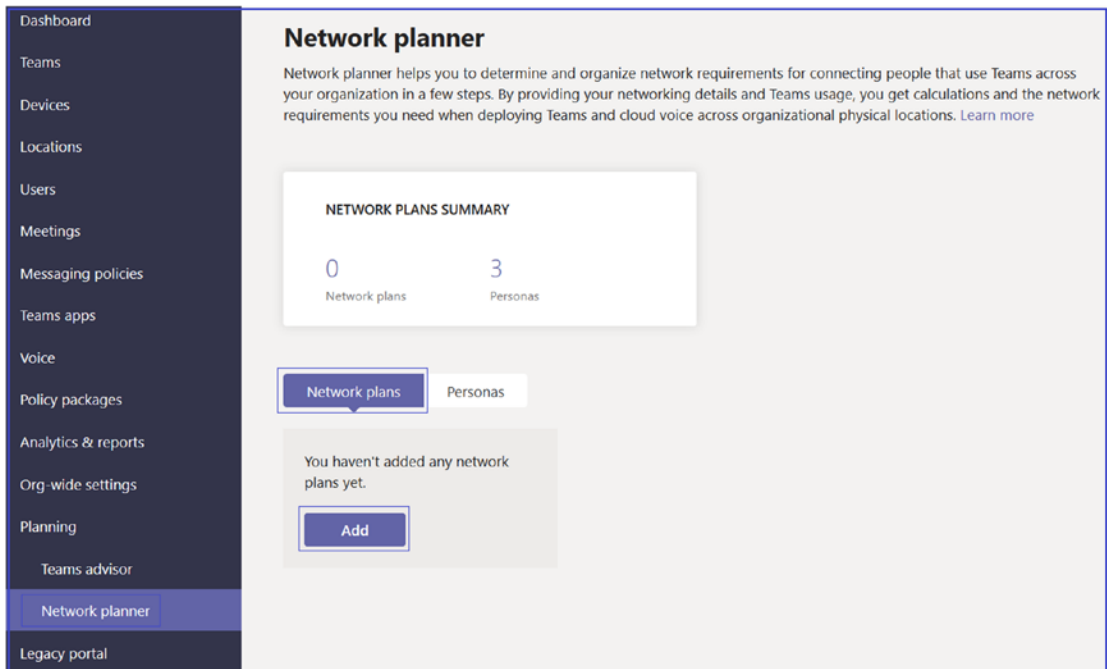


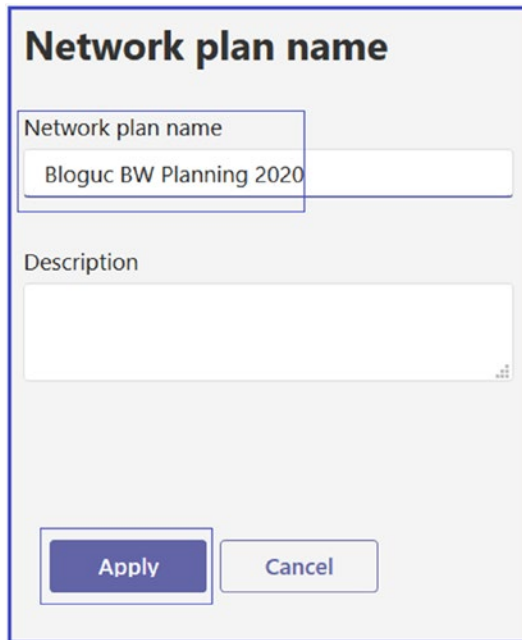
Figure 2-120. Network planner

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 Microsoft Teams admin center and then navigate to Planning and select Network Planner.
2. On the Network Planner page, under Network Plans, click Add, as shown in Figure 2-120.
3. On the Network Plan name page, enter the name for the network plan (e.g., Bloguc BW Planning 2020 in Figure 2-121), an optional description, and click Apply.



Network plan name

Network plan name

Bloguc BW Planning 2020

Description

Apply Cancel

Figure 2-121. 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 [2-122](#), click Save to commit the changes.

Bloguc HQ

This is HQ site

+ 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 2-122. 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 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 2-123.

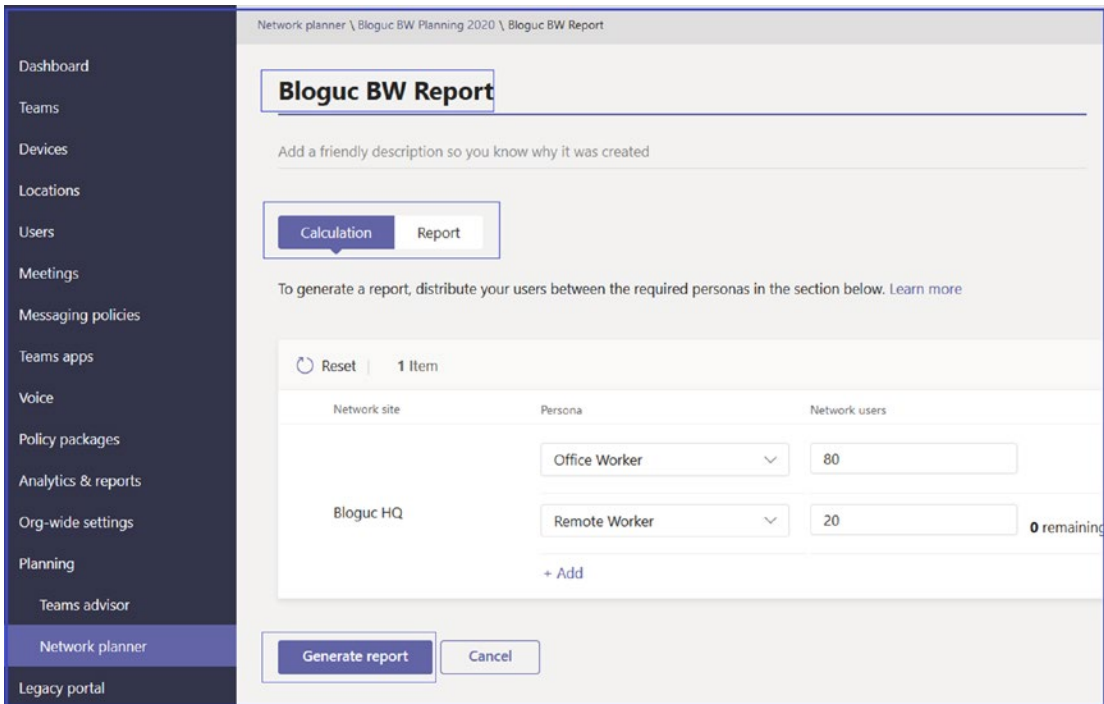


Figure 2-123. *Generating a report*

5. On the report page, review the report, including type of service, and required bandwidth for different services, such as audio, video, screenshare, Office 365 server traffic, and PSTN. Figure 2-124 shows the network planner report.

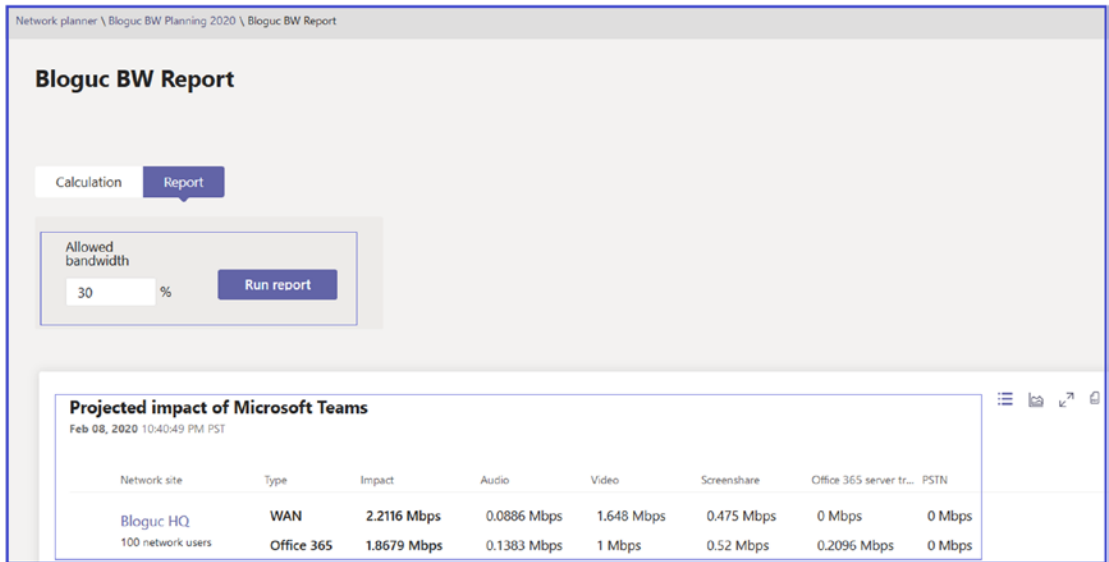


Figure 2-124. Network planner report

Legacy Portal

Legacy portal in this case means the Skype for Business Online portal. Previously most voice-related configuration was dependent on the legacy portal, but recently Microsoft has moved all configuration to the Teams portal. To access the legacy portal, log in to Teams admin center and navigate to Legacy Portal to open it (see Figure 2-125).

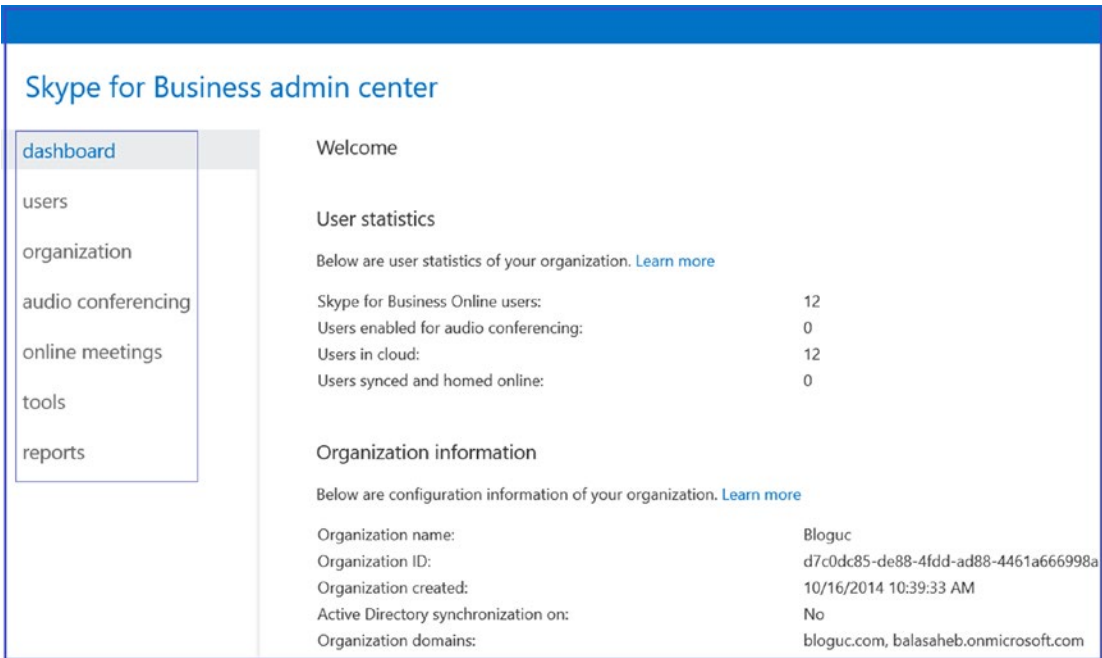


Figure 2-125. Legacy Skype for Business admin center

Call Quality Dashboard

Call Quality Dashboard (CQD) provides an overall view for analyzing Teams call quality. It supports Teams admin 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 on the audio and video call quality users are getting using Teams. It provides reports of call quality metrics that give you insights into overall call quality, server–client and client–client streams, and voice quality service-level agreements.

Using Call Quality Dashboard

Microsoft Teams has extensive reporting and analytical capabilities that help admins to measure overall call quality. When users report poor call quality, Teams and network admins can together check CQD to see if an overall site-related issue could be a contributing cause of the call quality problems. Microsoft has labeled first or second

many of the dimensions and measures. In the CQD the main logic determines which endpoint involved in the stream or call is labeled as first.

- First will always be considered Teams Cloud service because the Teams purely cloud-based 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.
- 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 Teams admin center, as well as directly by browsing to the CQD URL. Using Teams admin center, log in to Teams admin center and then navigate to and select Call Quality Dashboard. That will open a new browser tab for 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 2-126 shows the CQD displaying Overall Call Quality. You will see options to display Server–Client call quality, Client–Client call quality, and Voice Quality SLA.

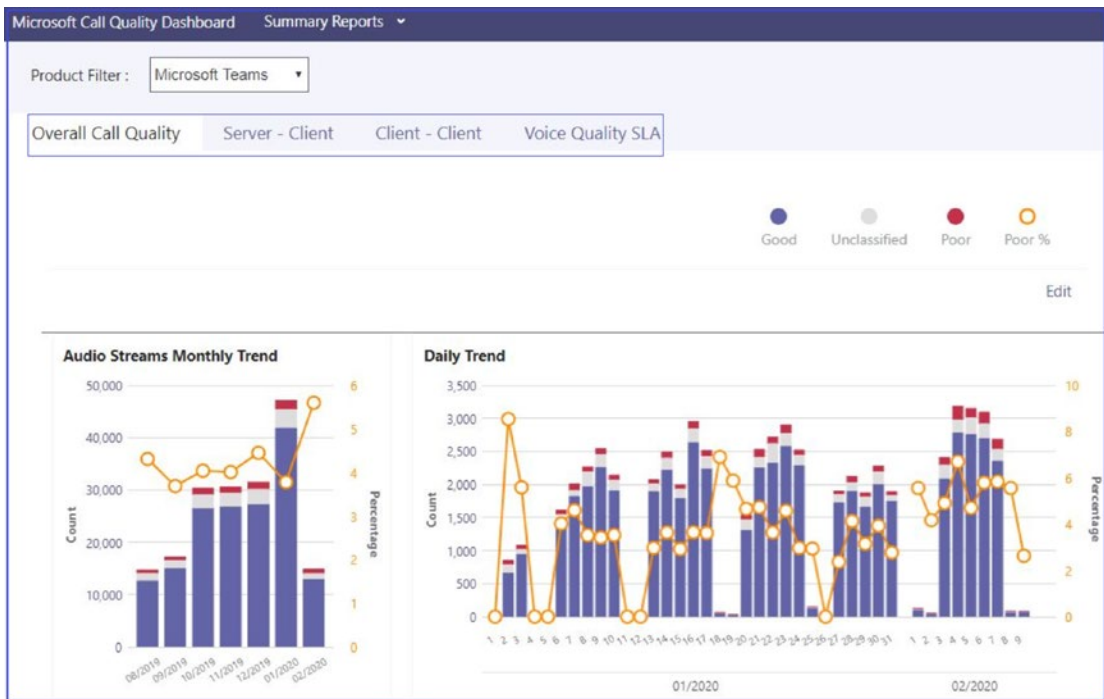


Figure 2-126. Call Quality Dashboard

You can see the CQD by directly browsing the URL at <https://cqd.teams.microsoft.com/spd/#/Dashboard>.

Displaying the List of Call Quality Reports

CQD provides multiple type of reports. Figure 2-127 shows the list of CQD reports on the Summary Reports tab. You can easily access each type of report by clicking on its report name. To see the summary report, log in to Teams admin center and then navigate to the CQD and then click it. It will open in a new browser tab.

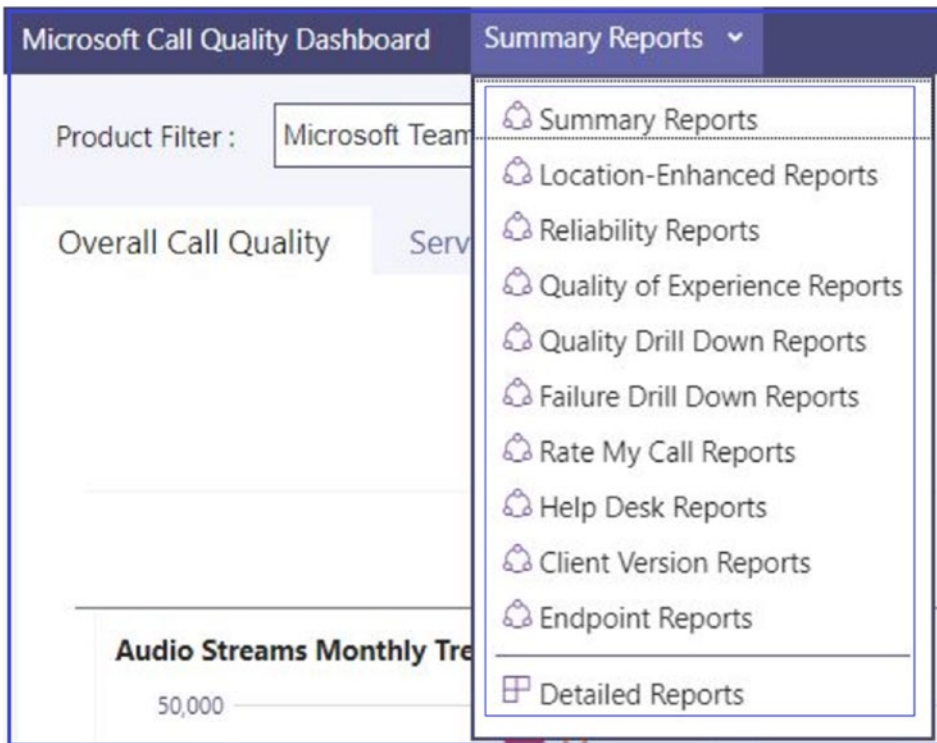


Figure 2-127. *Summary Reports tab*

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 2-128 shows an example of a detailed report.



Figure 2-128. 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 2-128 shows the monthly audio streams count ratio of and audio for the last seven months. There are no filters applied so the data reflect 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.

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 the 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.

Managing Microsoft Teams Identity

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.

Accessing Azure AD

To access Azure AD, log in to Microsoft 365 admin center by going through <http://portal.office.com/> and then clicking Admin or directly visiting the admin portal URL at <https://admin.microsoft.com/Adminportal/Home> or directly visiting the Azure AD admin center at <https://aad.portal.azure.com>.

Once the Microsoft 365 admin center page opens, click Show All to show all 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 2-129 shows the Azure AD admin center.

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.

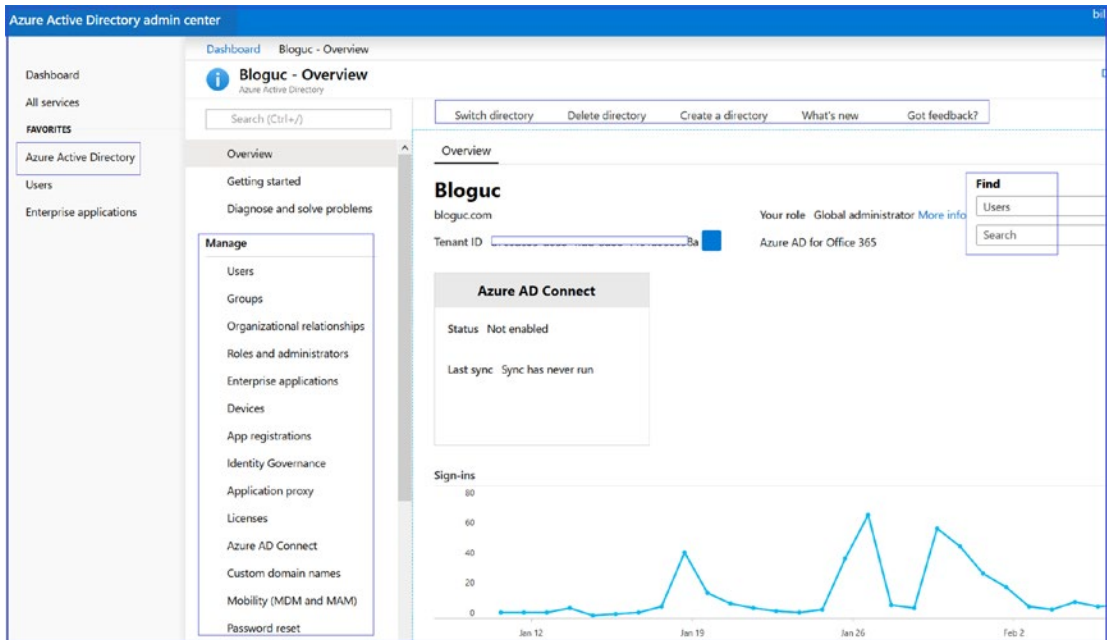


Figure 2-129. Azure Active Directory admin center

Microsoft 365 Admin Center

You can create users or Office 365 Groups and manage them through Microsoft 365 admin center. Figure 2-130 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 Microsoft 365 admin center here because Teams and add-on Phone System licenses are assigned and managed and Teams usage reports are available through Microsoft 365 admin center.

Accessing Microsoft 365 Admin Center

You can access Microsoft 365 admin center by going through <http://portal.office.com/> and clicking Admin or directly by visiting the admin portal URL at <https://admin.microsoft.com/Adminportal/Home>. You can use the Microsoft 365 admin center to assign Teams, Exchange, SharePoint licenses, and user management.

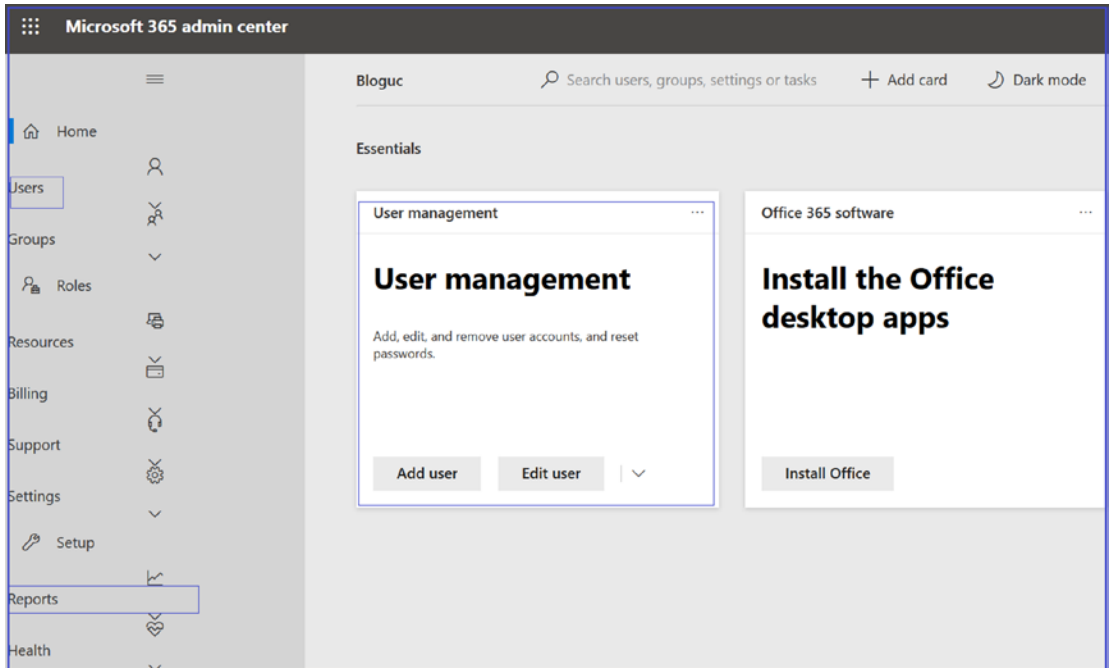


Figure 2-130. Microsoft 365 admin center

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

Teams usage 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 Microsoft 365

admin center you can view two activity reports: the Microsoft Teams device usage report and the Microsoft Teams user activity report [85].

1. To view the Teams user activity and device usage reports, log in to 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 2-131.

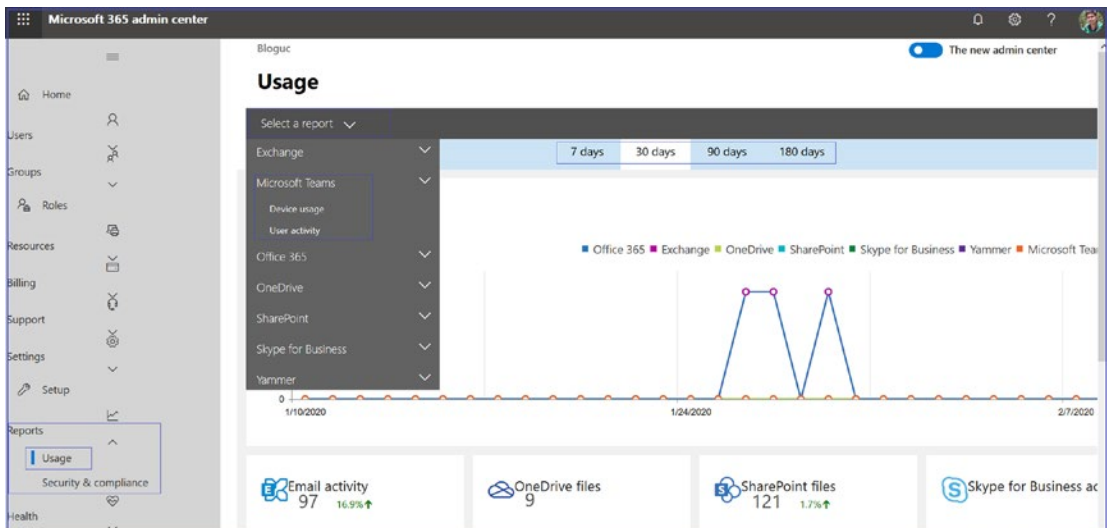


Figure 2-131. Teams usage reports

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

- Global administrator
- Exchange administrator
- SharePoint administrator
- Skype for Business 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)

Office 365 Security & Compliance Center

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 the all 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 hub a 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 the 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, application of data governance policies for the type of content that exists, the duration, and finally the ability to manage risks.

Understanding Identity and Access Management for Teams

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 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 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.

Accessing the Office 365 Security & Compliance Center

As a Teams admin and compliance and information security admin, you must be aware of what 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, shown in Figure 2-132. You can also directly access the Security & Compliance Center by visiting <https://protection.office.com/homepage>.

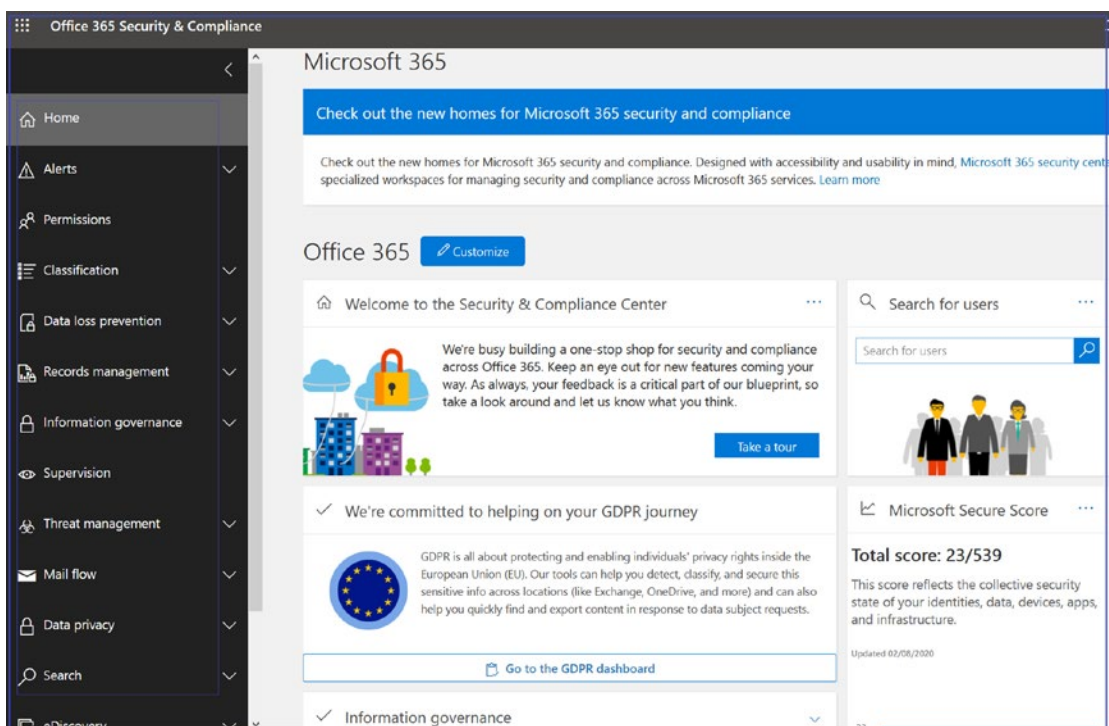


Figure 2-132. Office 365 Security & Compliance Center

Topics like managing sensitivity labels and data loss prevention policies, managing eDiscovery cases and supervision policies, configuring alert policies for events in Microsoft Teams, and how to create retention policies and information barriers are covered in Chapter 5.

Teams Management Through PowerShell

Windows PowerShell is one of the admin tools that you can use to handle most of your Teams management work through Windows PowerShell. Before using PowerShell, you need to install the Skype for Business Online module.

1. Download and install the Skype for Business Online Windows PowerShell module from <https://www.microsoft.com/en-us/download/details.aspx?id=39366>.

2. After installing the PowerShell module, connect PowerShell using a Teams administrator account name and password. First open Windows PowerShell run as administrator. Once the command prompt opens, run the following PowerShell commands (without MFA). See Figure 2-133.

```
Import-Module SkypeOnlineConnector
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession
```

3. With MFA run the following command:

```
Import-Module SkypeOnlineConnector
$sfbSession = New-CsOnlineSession
Import-PSSession $sfbSession
```

Note When it prompts, enter the login credential.

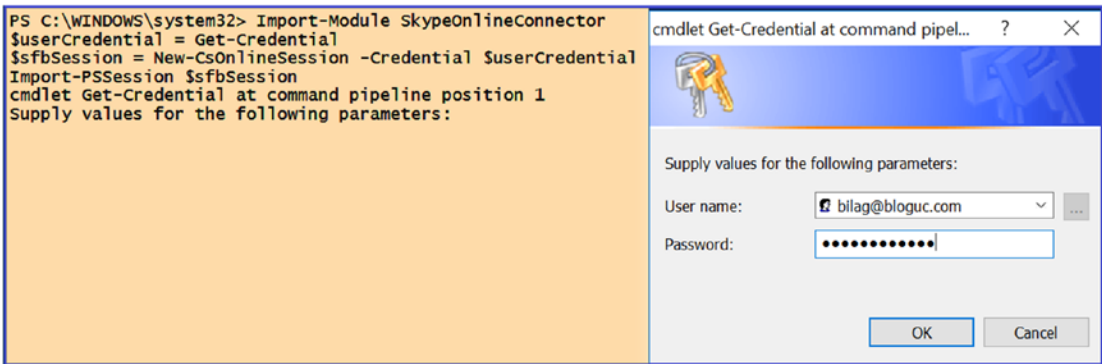


Figure 2-133. Importing Skype for Business Online module

4. Once you connect, you will be able to run Teams and Skype for Business PowerShell commands, as shown in Figure 2-134.

```

PS C:\WINDOWS\system32> Import-Module SkypeOnlineConnector
$UserCredential = Get-Credential
$SfbSession = New-CsOnlineSession -Credential $UserCredential
Import-PSSession $SfbSession
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:

ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_rf4brzpk.yde {Clear-CsOnlineTelephoneNumberReservation, ConvertTo-JsonForPsws, Disable-CsMeet...

PS C:\WINDOWS\system32> Get-CsTeamsMeetingConfiguration

Identity : Global
LogoURL : https://bloguc.com/wp-content/uploads/2018/06/logo_new.png
LegalURL : https://bloguc.com/legal.html
HelpURL : https://products.office.com/en-us/microsoft-teams/group-chat-software
CustomFooterText : Non-disclosure agreements may apply for all form of communication.
DisableAnonymousJoin : False
EnableQoS : True
ClientAudioPort : 50000
ClientAudioPortRange : 20
ClientVideoPort : 50020
ClientVideoPortRange : 20
ClientAppSharingPort : 50040
ClientAppSharingPortRange : 20
ClientMediaPortRangeEnabled : True

PS C:\WINDOWS\system32>

```

Figure 2-134. Connect and run Skype for Business Online and Teams commands

Note After connecting to the Skype for Business Online PowerShell module, you can run any Get, Set, or Grant PowerShell command. However, you cannot run Teams-specific commands like New, Get, or Set commands (e.g., Get-Teams, New-Team, etc.).

Now connect to the Microsoft Teams PowerShell command. First open Windows PowerShell as administrator. Once the command prompt opens, run the following PowerShell commands (without MFA). To install the Teams module and connect, run the following commands.

```

Install-Module MicrosoftTeams
Connect-MicrosoftTeams

```

After installing the Microsoft Teams module, connect to MicrosoftTeams module and then enter the credential and wait to connect, as shown in Figure 2-135.

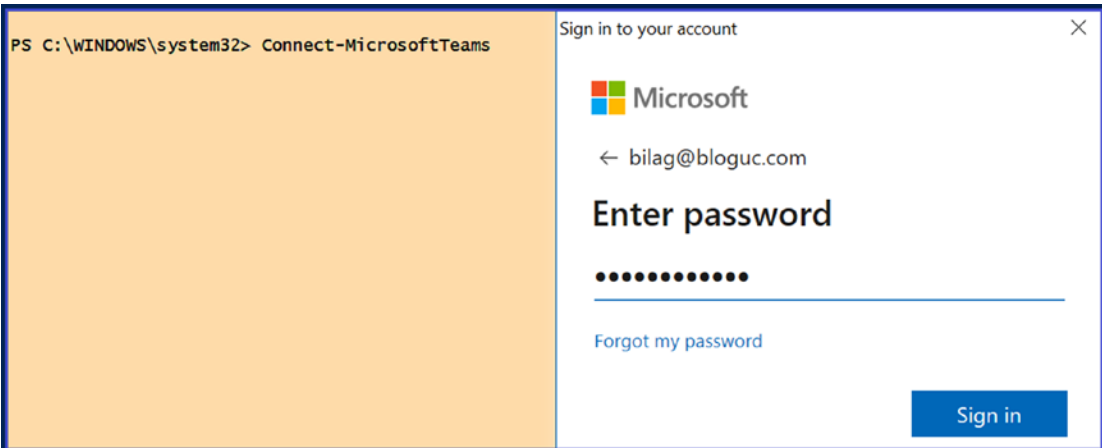


Figure 2-135. Connecting to Microsoft Teams PowerShell

After connecting to the Teams module, run the command to create a new team or channel. For example, Figure 2-136 shows new team creation using PowerShell.

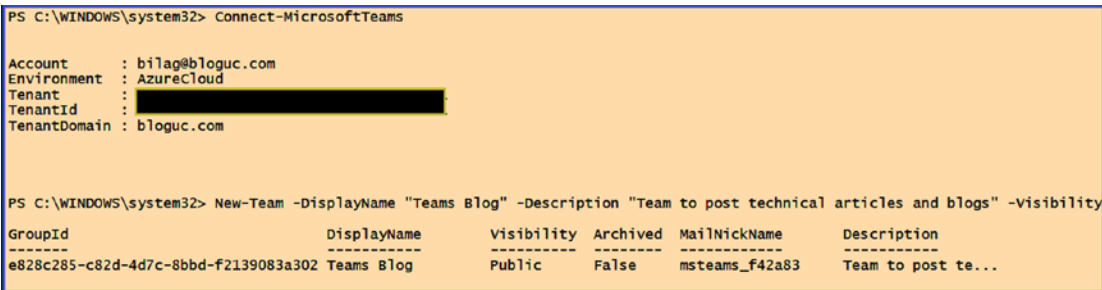


Figure 2-136. Creating a team using PowerShell

To learn more about Teams-specific commands, refer to <https://docs.microsoft.com/en-us/powershell/module/teams/new-team?view=teams-ps>.

Summary

In this chapter you learned about Teams authentication, managing and configuring MFA and conditional access for Teams, Teams client rollout, team and channel management, configuring and managing live events and Microsoft Stream, Teams management tools including Teams admin center, Azure AD, Microsoft 365 admin center and Security & Compliance Center, as well as Teams management through PowerShell. You also learned about the different management tools that are available with Teams, and the different clients that can work with Teams collaboration and communication.

CHAPTER 3

Organization Readiness for Microsoft Teams

Microsoft Teams offers multiple features, including audio and video calls, meetings, content sharing, real-time conversation, and so on. Microsoft did a commendable job by building Teams from scratch with the latest codec and media stack support. Additionally, Teams does provide optimal call quality; however, it requires a network infrastructure ready to handle Teams signaling and media traffic seamlessly, and provide sufficient bandwidth for Teams audio and video media traffic. Teams is designed to provide optimal call quality, but if your infrastructure is not provisioned correctly and not ready for Teams, then Teams will not work the way it should, and ultimately the end users suffer.

Preparing the infrastructure is therefore important. Before starting Teams deployment, you as a Teams admin must ensure that all Teams network requirements are completed, including infrastructure and network readiness. You can then plan for starting the actual deployment. Microsoft did a better job of consolidating all the Teams (Office 365) IP subnets and port and protocol requirements in one document (<https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#skype-for-business-online-and-microsoft-teams>) you can refer to in completing these requirements.

So far, you have learned about Teams fundamentals, team and channel architecture, live events, identity, and Teams management tools. This chapter covers detailed information on network assessment and bandwidth planning for Teams, how to deploy and manage QoS, and how to deploy a virtual private network (VPN) split tunnel for Microsoft Teams media traffic. Before the deployment of Microsoft Teams in a production environment, you, as an admin, need to determine if the existing network meets the networking requirements of Microsoft Teams. Make sure that you have the

required bandwidth, access to all required IP addresses, and the correct ports opened. You also need to make sure you are meeting the performance requirements for Teams real-time media traffic such as audio, video, and application sharing [14].

Network Assessment and Bandwidth Planning for Teams

Before doing a network assessment and bandwidth planning for Microsoft Teams, you must know what different types of traffic Teams generates. At a high level, Teams produces and supports two types of traffic: Teams signaling traffic, also known as gesturing, and Teams media traffic, known as real-time media traffic. Teams is a purely cloud-hosted service that allows it to operate in three types of network traffic directions.

- *Teams signaling traffic:* Teams data traffic between the Teams service (Office 365 Online environment) and the Teams client for signaling, presence, chat, file upload and download, and OneNote synchronization).
- *Teams media traffic:*
 - Teams one-to-one real-time communications media traffic for audio, video, and application (desktop) sharing.
 - Teams conferencing real-time media communications traffic for audio, video, and application (desktop) sharing.

If any of the Teams network traffic directions are affected, then it will affect Teams communication. Teams traffic flows between the Teams clients directly in one-to-one call situations or between the Office 365 environment and the Teams clients for meetings.

To ensure the optimal traffic flow for Teams one-to-one and conference scenarios, you as an admin must allow seamless traffic flow between your organization's internal network segments, such as between sites over the wide-area network (WAN) as well as between the network sites and Office 365 environment. For example, the Bloguc Organization has central offices in Tracy, CA, and Denver, CO, and branch offices in India. We allowed traffic between central and branch offices over WAN without any block, and these offices directly talk to Teams services (Office 365) using the Internet. Also, we allowed all Teams IP subnets, ports/protocol, including FQDN and URLs, so there will be no interference in traffic flow.

Note Actively blocking specific ports or not opening the correct ports will lead to a degraded Teams experience.

Carrying Out a Network Assessment Before Teams Deployment

You have learned what type of traffic Teams generates, the traffic directions, and how it potentially affects the user experience. A network assessment is essential before Teams deployment because it will evaluate the existing network infrastructure and pinpoint the network impairments that could cause poor call quality. Also, the assessment will identify the performance-linked problems that can be introduced into the environment through latency and packet loss. Issues such as these will result in a negative experience in Teams audio and video scenarios, where real-time streams are essential.

Network assessment has several different aspects.

- It assesses the existing network configuration that might affect Teams traffic, while evaluating the existing network environment for hard limitations such as blocked IP addresses, faulty name resolution through DNS, and blocked ports. These problems are easy to spot because specific Teams features will simply not work at all when IP addresses or ports are blocked.
- Point-in-time problems, like bandwidth, latency, or packet-loss issues, are more complicated, because they might appear only under special conditions; for example, if the Bloguc Organization HQ office has a high number of users that are using audio and video communication at the same time. Thus, when planning the network requirements for a Teams deployment, you must calculate the maximum number of concurrent users, including a sufficient buffer and bandwidth.

There are several best practices for preparing your environment for Microsoft Teams.

- You must allow seamless connectivity from your corporate network where the user resides to Microsoft Teams service, which is in Office 365. Also, make sure that all required DNS names are resolved correctly, and Teams service IP addresses must be reachable.
- Make sure the network connection quality of an established connection is optimal through measuring in values, such as latency, jitter, and packet-loss rates. Also, the existing networking hardware must provide a stable connection with minimum network hop by keeping as few active networking devices between a Teams client and Office 365 as possible. Each active networking device adds additional latency and raises the chance of connectivity quality issues. So, optimizing network path by eliminating the unnecessarily network devices or hop, will expedite packet flow and untimely improve call quality.
- Make sure to keep enough bandwidth available for Teams communication to Office 365 services. Remember, the required bandwidth of Teams depends on the required functionalities and number of Teams clients in an organization location. You must analyze the maximum number of concurrent participants and then multiply this number with the provided utilized Teams functionalities. For example, Bloguc has 100 users in the HQ office, and the available bandwidth is 100 MB. At any point in time 30 users will be on calls, so the available bandwidth must be sufficient for 30 users' calls.
- The Teams client can be connected over any network, either wired or wireless. Teams clients connected over a wireless connection, such as corporate Wi-Fi networks and hotspots are more vulnerable for high latency and possibly higher packet loss because wireless networks usually are not necessarily designed or configured to support real-time media or not prepared for real-time services, such as Teams audio and video communication. For the wireless network, implementing QoS or Wi-Fi Multimedia (WMM) will ensure that media traffic is getting prioritized appropriately over the Wi-Fi networks. You can work with your organization network engineer to plan and optimize the Wi-Fi bands and access point placement.

Implement band steering and ensure the access points that are next to each other are on channels that do not overlap. Furthermore, the network coverage must provide enough bandwidth even between wireless access points and on the edges.

- One of the significant network impairments is the intrusion detection system (IDS) and intrusion prevention system (IPS) feature on the firewalls that can analyze the payload of data packages for the attack signatures. If any organization network environment uses IDS and IPS solutions, then make sure all network traffic between your organization and the Teams services (Office 365) is whitelisted and excluded from any kind of scanning.
- Another best practice for Network Address Translation (NAT) pool size provides access to multiple internal systems by using a single public IP address. When multiple users and devices access Office 365 using NAT or Port Address Translation (PAT), you, as a Teams admin, must ensure that the devices hidden behind each publicly routable IP address do not exceed the supported number. You might need to check with your network engineer, who can help you to understand NAT configuration.
- Most of the time, the organization uses VPN that offers an encryption tunnel between endpoints, like remote users and the corporate network. Generally, VPNs are not designed to support real-time media traffic and introduce an extra layer of encryption on top of media traffic that is already encrypted. This adds overhead. Additionally, connectivity to the Teams service (Office 365) might not be efficient due to hair-pinning traffic through a VPN device. For VPNs, the suggestion is to provide an alternate path that bypasses the VPN tunnel for Teams traffic. This is generally known as split-tunnel VPN. We will cover the VPN split tunnel in detail in this chapter.
- Finally, verifying overall network health is equally critical, so identify the network health and quality baseline before Teams deployment in your organization. After planning on the Teams implementation in your organization using the existing network, you should ensure there is sufficient bandwidth, accessibility to all required IP addresses, correct configuration of ports, and meeting the performance requirements for Teams real-time media [14a].

Network Bandwidth Requirements for Microsoft Teams Calling Scenarios

So far, you have learned about network assessment and network best practices. Next, you need to understand the importance of network quality between your organization’s network and Microsoft Teams cloud service and the required bandwidth for each Teams calling scenario. When assessing the existing network environment, first complete Teams IP address, port/protocol, URLs, and faulty name resolution through DNS requirements, because specific Teams features will not work at all when Teams service IP addresses or ports are blocked. Additionally, finding the bandwidth, latency, or packet-loss issues is more complicated because they might appear only under particular circumstances. Refer to Table 3-1, which shows the recommended network capabilities and accepted latency, burst packet loss, packet loss, jitter, and packet reordering. For example, Teams call quality will be best when you have less than 50 ms latency between your organization network and Microsoft Edge router along with packet loss and jitter values under the limit.

Table 3-1. Accepted Limits for Network Values [14a]

Network (Value)	Teams client to Microsoft Edge N/W (without SfB Hybrid)	Customer Edge N/W to Microsoft Edge (with SfB Hybrid)
Latency (one way)	< 50ms	< 30ms
Latency (RTT or Round-trip Time)	< 100ms	< 60ms
Burst packet loss	<10% during any 200ms interval	<1% during any 200ms interval
Packet loss	<1% during any 15s interval	<0.1% during any 15s interval
Packet inter-arrival Jitter	<30ms during any 15s interval	<15ms during any 15s interval
Packet reorder	<0.05% out-of-order packets	<0.01% out-of-order packets

Because Microsoft Teams supports multiple features, each feature has different bandwidth requirements; for example, Teams one-to-one audio calling requires 30 kb bandwidth for upstream and downstream. Table 3-2 shows call scenarios and required network bandwidth for your Teams clients to optimally use Teams features.

Table 3-2. *Teams Call Scenarios with Required Bandwidth [14a]*

Teams call/ conference scenarios	Required Bandwidth (up/down)
One-to-one audio calling	30 kbps
One-to-one audio calling and screen sharing	130 kbps
One-to-one video calling with resolution 360p at 30fps	500 kbps
One-to-one High Definition (HD) quality video calling with resolution of HD 720p at 30fps	1.2 Mbps
One-to-one HD quality video calling with resolution of HD 1080p at 30fps	1.5 Mbps
Group (more than 2 participant) Video calling	500kbps/1Mbps
HD Group video calling (540p videos on 1080p screen)	1Mbps/2Mbps

For network assessment, you can use the Network planner and Network Testing Companion tools.

Network Planner

Using Network planner, an admin can create representations of an 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 the Network planner, you must have global administrator, Teams admin, or Teams communication administrator role permissions.

Adding a Plan

You can access the Network planner tool, shown in Figure 3-1, by going to Microsoft Teams admin center and navigating to Planning. Select Network Planner.

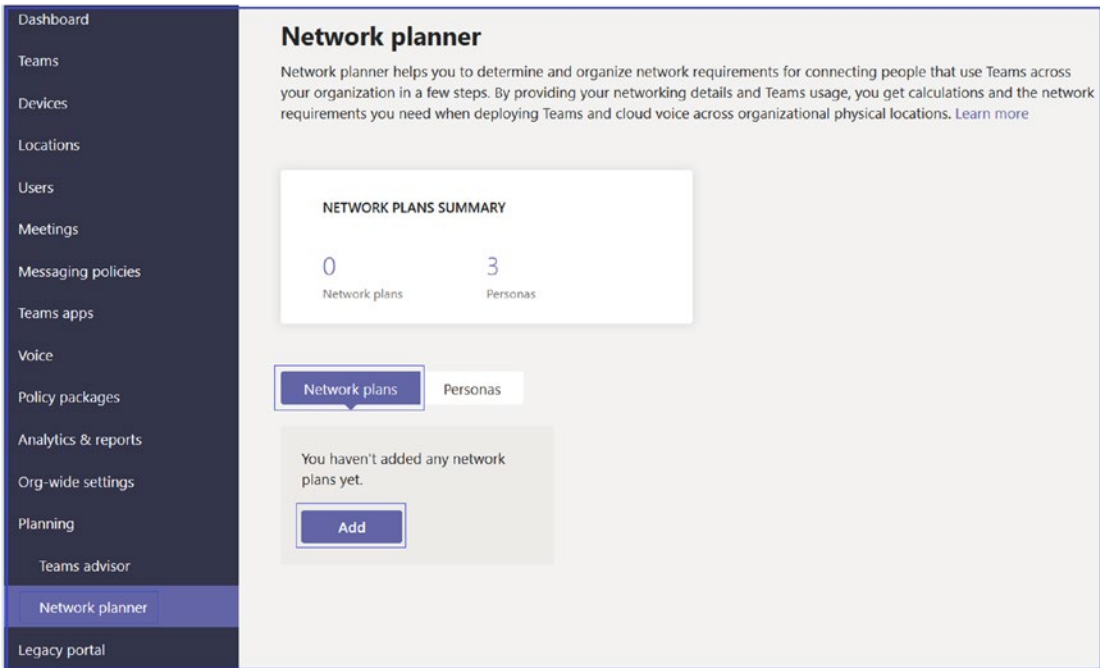


Figure 3-1. Network planner

When you click Add, it will allow you to create a Network planner name. By default, there will be three user personas; you can add custom personas on the Network Planner page by clicking the Users tab. 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.

Developing a Network Planner Plan

The 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 Microsoft Teams admin center and then navigate to Planning. Select Network Planner.
2. On the Network Planner page, under Network Plans, click Add.

3. On the Network Plan Name page, enter the name for the network plan (in the example shown in Figure 3-2, Bloguc BW Planning 2020) and an optional description. Click Apply.

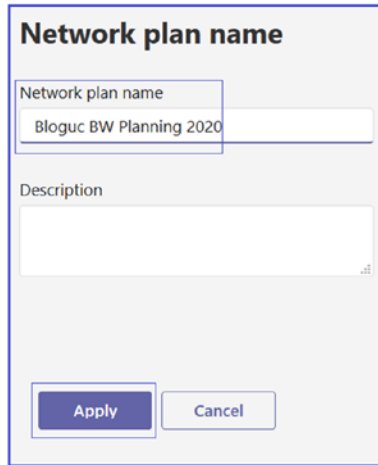
The image shows a web form titled "Network plan name". It has two input fields: "Network plan name" with the text "Bloguc BW Planning 2020" entered, and "Description" which is currently empty. At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 3-2. *Adding 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, click Add A Network Site. On the Add A Network Site page, shown in Figure 3-3, 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 the details, click Save to commit the changes.

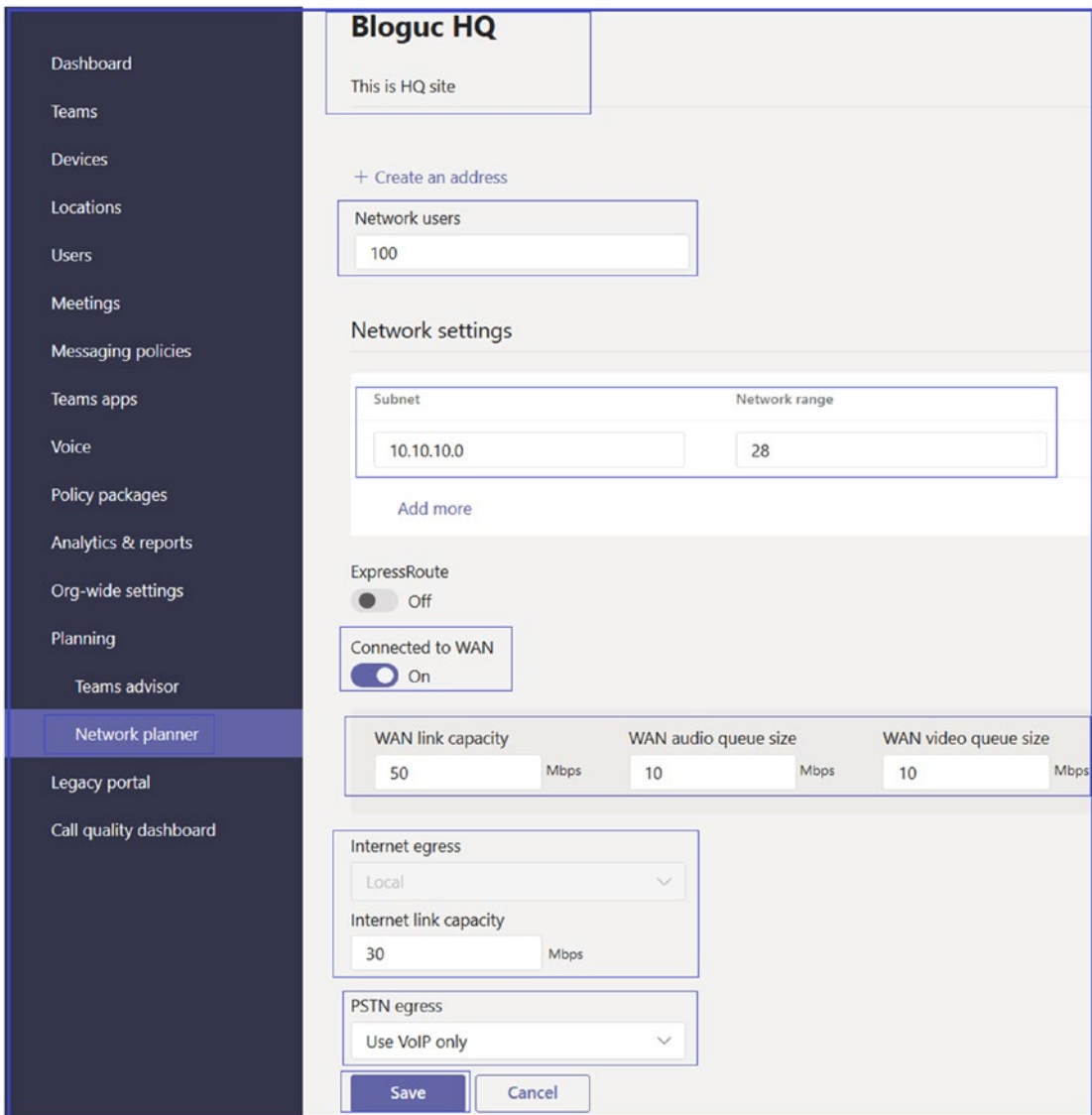


Figure 3-3. Adding a network site and subnet

After creating a plan, the next thing you have to do is create a report based on your network plan and view the projected impact of Teams media traffic such as audio, video, meetings, and PSTN calls. To do so, log in to Teams admin center, navigate to Planning, and then select Network Planner. On the Network Planner page, in the Network Plans section, select your network plan (given a meaningful name). On the plan page, select Report, and then click Add Report.

On the Add Report page, enter the report name (Bloguc BW Report in our example), and in the Calculation section, select the type of persona, such as Office Worker or Remote Worker and the number of each persona type, and then click Generate Report. On the report page, review the report including type of service, and required bandwidth for different services, such as audio, video, desktop sharing, Office 365 server traffic, and PSTN.

Network Testing Companion Tool

You can check your network quality before or after a Teams meeting using the Network Testing Companion tool. Microsoft Teams and Skype for Business Online are both cloud-based applications, which means for Teams and Skype for Business Online, both clients register against cloud services and leverage rich Office 365 cloud services to provide an optimal experience for audio and video calling, meetings, chat, and many more features. To provide optimal call quality, your network must be well prepared for Teams and Skype for Business Online traffic without any blockages. To check network quality and make assessments, admins need a tool that will help to check network quality. That is where the Network Testing Companion tool comes in handy. It gives you an easy way to test your network quality and your connection to Microsoft Teams or Skype for Business Online. The results can be easily interpreted and shared with network administrators to gain insights into potential network issues.

The Network Testing Companion tool is not only useful to troubleshoot audio and video quality issues; it is also very helpful in the planning phase of a Microsoft Teams deployment. I would recommend using this tool to check your network connection before you make an audio or video call or after you've had a poor-quality experience in a Teams meeting.

Prerequisites for the Network Testing Companion Tool

There are some prerequisites for this tool. Your operating must be Windows 7 or later, you must have Windows Management Framework 5.1 installed, and most important, you must have a local Administrator account permission to install the Network Testing Companion tool.

Installing the Network Testing Companion Tool

Installation is very straightforward; however, to install this tool, a user must have administrator rights to the computer. You can refer to below PowerShell command details.

To install this tool on the local computer, go to Start, and then enter PowerShell. Right-click Windows PowerShell, and then select Run As Administrator. Then enter the following command, as shown in Figure 3-4:

```
Install-Module -Name NetworkTestingCompanion
```

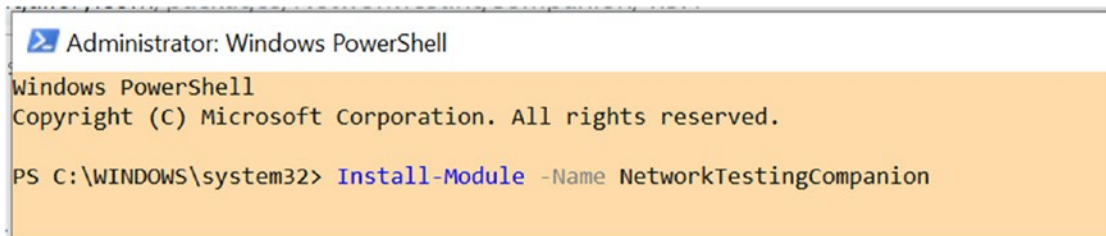


Figure 3-4. *Installing the Network Testing Companion tool*

You'll need to enter Y (Yes) at two prompts, one for the NuGet provider and one to accept the repository's being untrusted. After the PowerShell module has been installed, create shortcuts for opening the tool. Type the following command, and then press Enter:

```
Invoke-ToolCreateShortcuts
```

After installation, to start the Network Testing Companion tool, select the icon on your desktop or Start menu.

Note The Network Testing Companion tool uses Windows PowerShell. If your computer's execution policy doesn't permit you to run scripts, the command for creating shortcuts won't work even if the module was installed successfully. Refer to the Execution policy documents for an alternate option: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-6.

Using the Network Testing Companion Tool

This tool is self-explanatory. After you install this tool, you can simply open it by clicking Start and then typing Network Testing Companion in the search box. Once this tool opens, it will look like Figure 3-5. This tool might take some time to check your Internet connection, the headset you are using, your operating system, and network assessment tool.

Once this tool opens, you can click Start in the test pane; the tool will perform a connectivity check against the Microsoft Transport Relay network, making sure all the IP addresses and required ports are reachable. If any single IP address or port is unreachable, the test is considered to have failed, and a red X is displayed under Connectivity on the Start Tests tab in the test pane; if the connectivity test passes, a green check mark is displayed. After the connectivity test, the companion runs audio quality tests [14].

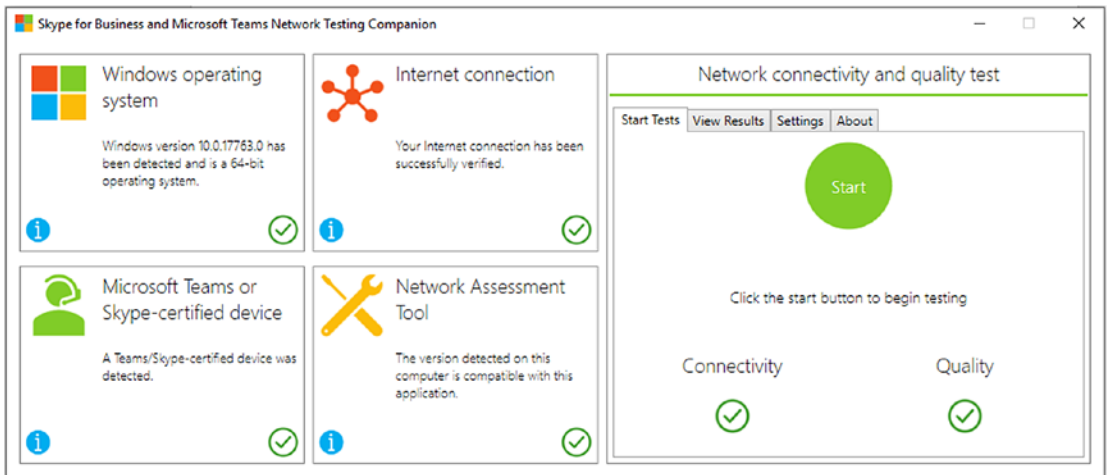


Figure 3-5. Network Testing Companion tool

If all audio quality test results are within limits, a green check mark is displayed under Quality on the Start Tests tab in the test pane. If any of the tests fail, a red X is displayed. You will get detailed reports about the connectivity and quality test results on the View Results tab, shown in Figure 3-6.

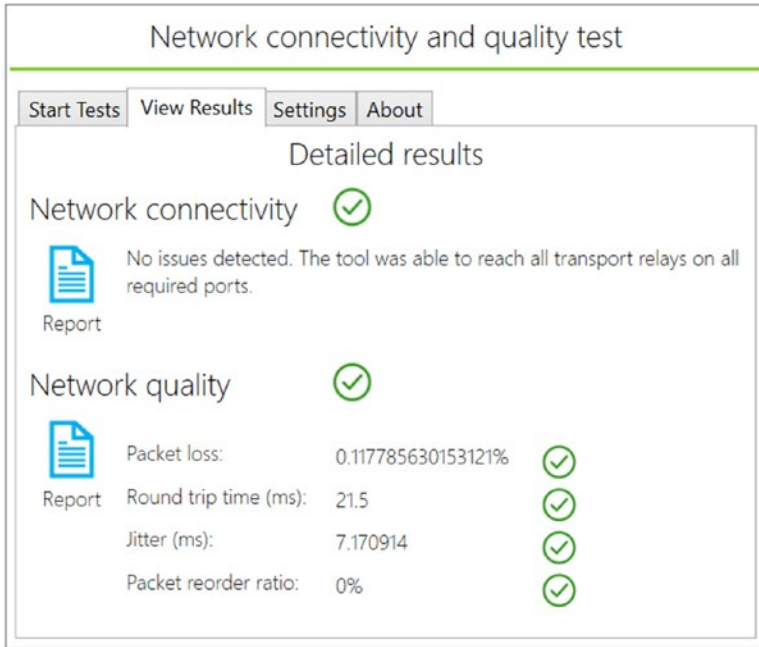
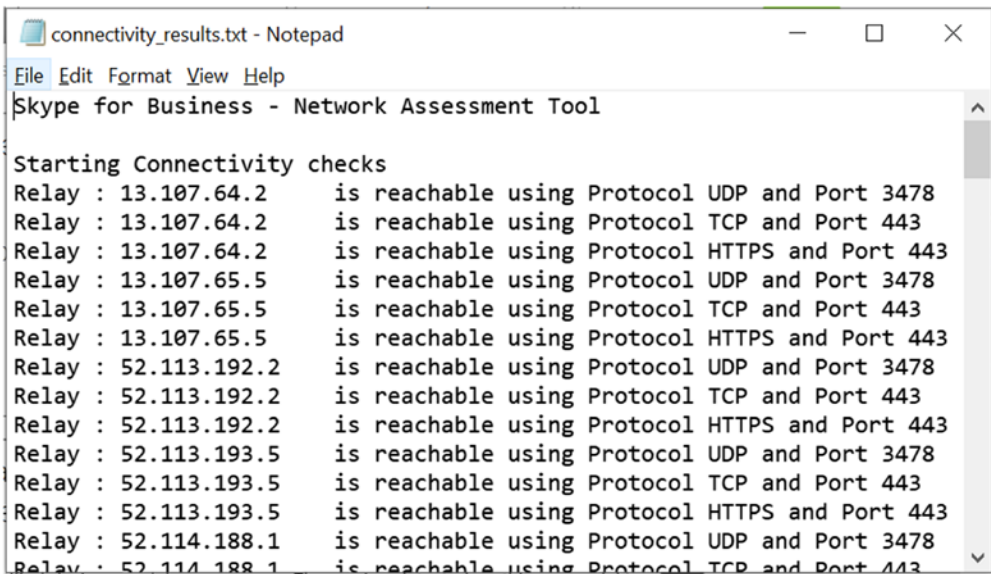


Figure 3-6. Network connectivity and quality test

Select the Network Connectivity Report icon to open a list of all the connectivity checks performed by the companion. If any replay IP address is not reachable, then it will show connectivity issues. Figure 3-7 shows IPs and ports are reachable.



```

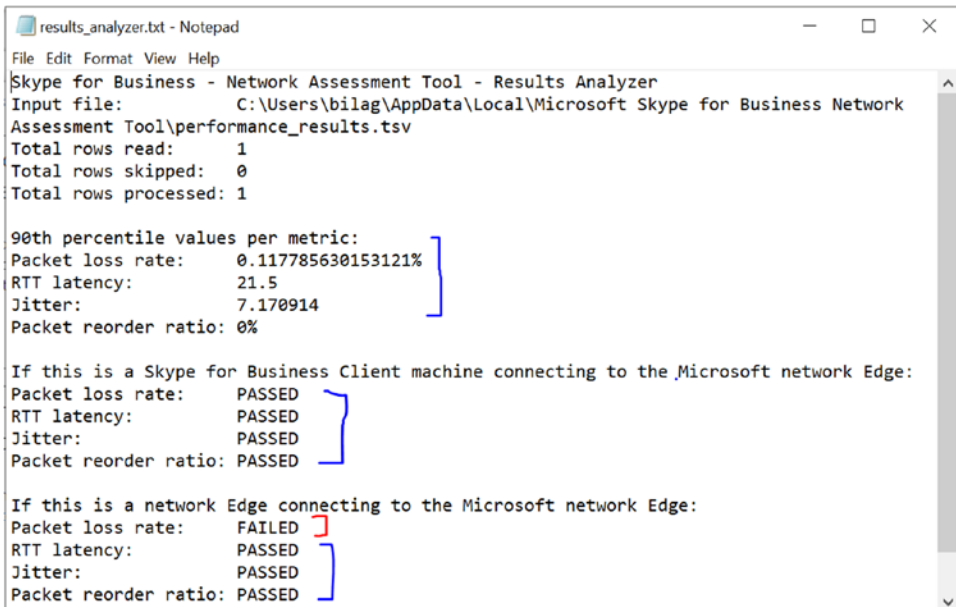
connectivity_results.txt - Notepad
File Edit Format View Help
Skype for Business - Network Assessment Tool

Starting Connectivity checks
Relay : 13.107.64.2      is reachable using Protocol UDP and Port 3478
Relay : 13.107.64.2      is reachable using Protocol TCP and Port 443
Relay : 13.107.64.2      is reachable using Protocol HTTPS and Port 443
Relay : 13.107.65.5      is reachable using Protocol UDP and Port 3478
Relay : 13.107.65.5      is reachable using Protocol TCP and Port 443
Relay : 13.107.65.5      is reachable using Protocol HTTPS and Port 443
Relay : 52.113.192.2     is reachable using Protocol UDP and Port 3478
Relay : 52.113.192.2     is reachable using Protocol TCP and Port 443
Relay : 52.113.192.2     is reachable using Protocol HTTPS and Port 443
Relay : 52.113.193.5     is reachable using Protocol UDP and Port 3478
Relay : 52.113.193.5     is reachable using Protocol TCP and Port 443
Relay : 52.113.193.5     is reachable using Protocol HTTPS and Port 443
Relay : 52.114.188.1     is reachable using Protocol UDP and Port 3478
Relay : 52.114.188.1     is reachable using Protocol TCP and Port 443

```

Figure 3-7. Connectivity test results

Select the Network Quality Report icon for a summary of results for the audio quality tests of packet loss rate, round-trip time, jitter, and packet reorder ratio. The report, shown in Figure 3-8, also summarizes whether the test results pass or fail network performance requirements.



```

results_analyzer.txt - Notepad
File Edit Format View Help
Skype for Business - Network Assessment Tool - Results Analyzer
Input file:          C:\Users\bilag\AppData\Local\Microsoft Skype for Business Network
Assessment Tool\performance_results.tsv
Total rows read:     1
Total rows skipped:  0
Total rows processed: 1

90th percentile values per metric:
Packet loss rate:    0.117785630153121%
RTT latency:         21.5
Jitter:              7.170914
Packet reorder ratio: 0%

If this is a Skype for Business Client machine connecting to the Microsoft network Edge:
Packet loss rate:    PASSED
RTT latency:         PASSED
Jitter:              PASSED
Packet reorder ratio: PASSED

If this is a network Edge connecting to the Microsoft network Edge:
Packet loss rate:    FAILED
RTT latency:         PASSED
Jitter:              PASSED
Packet reorder ratio: PASSED

```

Figure 3-8. Results analyzer

Figure 3-8 shows the all metrics are under their limits; however, some packet loss was reported, and that is why the packet loss rate shows as failed.

Deploying and Managing Quality of Service

Microsoft Teams provides real-time communication, including persistent chat, audio and video calls (VoIP), conferences, desktop sharing, PSTN calls, content sharing, and so on. These capabilities, however, will increase the traffic on your existing network. It is increasingly important for you as a Teams admin to balance network performance with QoS. All of these modalities include signaling and media traffic, and this real-time traffic is latency sensitive. Microsoft Teams is a latency-sensitive application; to provide an optimal user experience using Teams audio, video, and application sharing, you must prioritize the Teams real-time media traffic against lower priority traffic.

There are different ways to prioritize network traffic, but the most common way is by using Differentiated Services Code Point (DSCP) markings. DSCP values can be applied or tagged based on port ranges and via Group Policy objects (GPOs). Because Microsoft Teams is available across the platform, including Windows, macOS, iOS, Android, and so on, applying port ranges via GPO will not work for non-Windows devices. It is a best practice that you use DSCP tagging based on port ranges on the network layer because it will work for all devices, including macOS, iOS, and Android devices. In fact, a combination of GPOs for Windows and DSCP tagging at the network layer will work better.

QoS is more beneficial when you configure it from end to end, meaning from the user computer to network switches to routers to the cloud (Office 365 Service), because any part of the path that fails to support QoS can degrade the quality of the entire call [99].

Microsoft Teams is a cloud-only service, so you don't have end-to-end control on the network. When network traffic leaves your management network, you will be dependent on the Internet, where you don't have much control. Basically, the interconnect network will be an unmanaged network Internet connection, illustrated in Figure 3-9. One option available to address end-to-end QoS is Microsoft Azure ExpressRoute, which requires an additional investment.

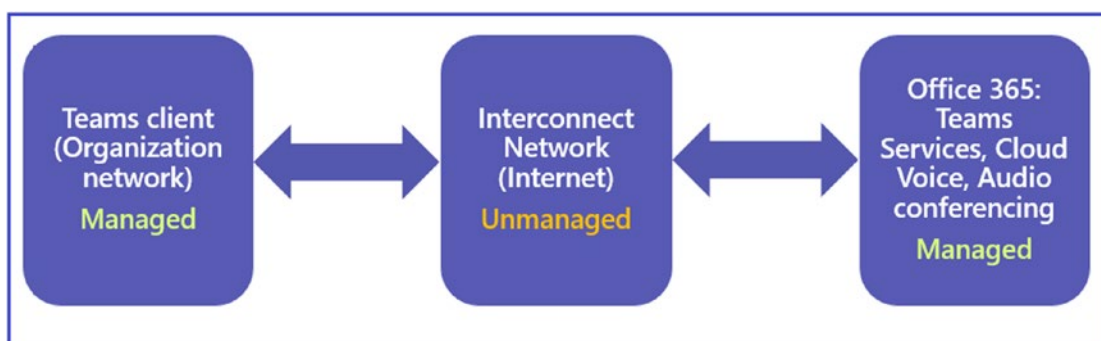


Figure 3-9. *Managed and unmanaged network*

Even though you will not have end-to-end control on the network, it is highly recommended that you implement QoS on the portion of the network that you have control over, that is your on-premises network. This will increase the quality of real-time communication workloads throughout your deployment and improve chokepoints in your existing deployment.

Deploying Quality of Service for Microsoft Teams

For Teams traffic, you should use GPO and DSCP marking using port ranges to accommodate Windows and non-Windows devices. This guide only covers the QoS configuration at the endpoint level as well as the network layer. It is best practice to use a GPO to grab the majority of clients, and also use port-based DSCP tagging to ensure that mobile, Mac, and other clients will still get QoS treatment (at least partially).

Table 3-3 shows the DSCP values and client source port ranges that are recommended for Microsoft Teams media traffic.

Table 3-3. *Teams Media Category with Client Source Port Ranges [99]*

Client Source Port Range	Protocol	Media Category	DSCP Value	DSCP Class
50,000–50,019	TCP/UDP	Audio	46	Expedited Forwarding (EF)
50,020–50,039	TCP/UDP	Video	34	Assured Forwarding (AF41)
50,040–50,059	TCP/UDP	Application/ Desktop Sharing	18	Assured Forwarding (AF21)

Applying DSCP Marking at Network Layer

To implement DSCP marking on network devices, you as a Teams admin need to work with network engineers to configure port-based DSCP tagging by using access control lists (ACLs) on network devices (switches and routers; basically the network engineer will configure devices to mark the Teams audio, video, and application sharing traffic at the ingress/egress routers typically located on the WAN based on the client source port ranges defined for each modality. Although this works across platforms, it only marks traffic at the WAN edge, not all the way to the client computer; therefore, this incurs management overhead.

To set this up, you can discuss and share Teams client source port ranges with DSCP class and value with your network engineer.

DSCP Marking at Endpoint Level Using Policy-Based QoS

QoS policies are applied to a user login session or a computer as part of a GPO that you have linked to an Active Directory container, such as a domain, site, or organizational unit (OU). QoS traffic management occurs below the application layer, which means that your existing applications do not need to be modified to benefit from the advantages that are provided by QoS policies.

For Microsoft Teams, we need to set up QoS policies for computer configuration so that whoever logs in to a computer and uses the Teams client will have the policy applied [99a].

The following is the GPO path: *Default Domain Policy* ► *Computer Configuration* ► *Policies* ► *Windows Settings* ► *Policy-Based QoS*

Follow these steps to implement policy-based QoS for Teams.

1. First, define the Teams client source port ranges on the Teams admin center modern portal. Log in to Teams admin center, then go to a meeting and then meeting settings under Network.

URL: <https://admin.teams.microsoft.com/policies/meetings>

- a. Turn on “Insert Quality of Service (QoS) markers for real-time media traffic,” refer the below image.
- b. Select “Select a port range for each type of real-time media traffic,” refer the below image.

- c. Update starting and ending port ranges with media traffic type.
Refer the figure 3-10, which shows the media port ranges.

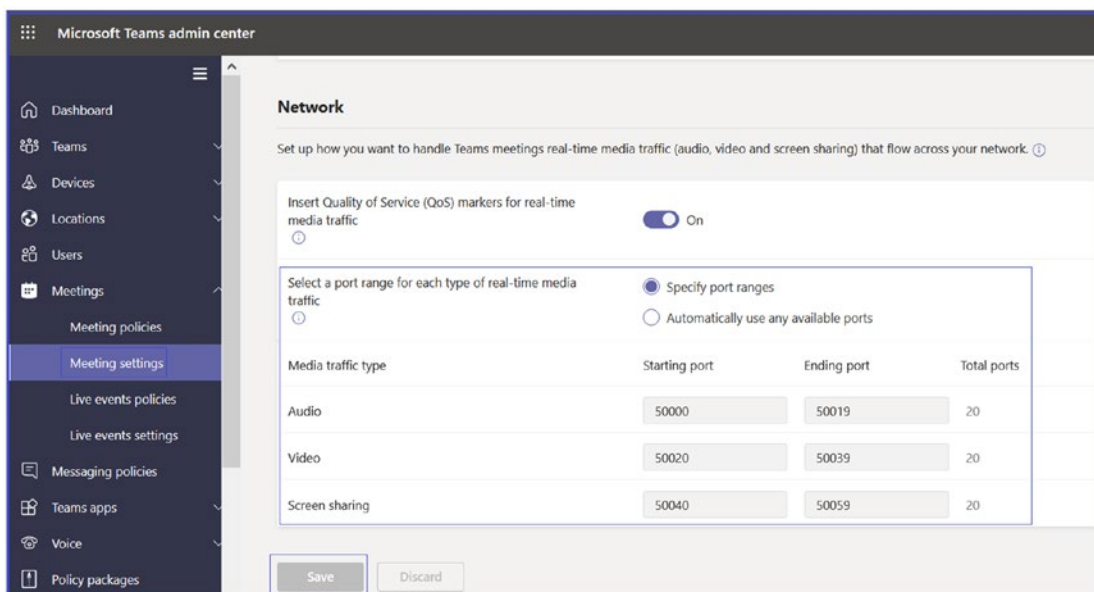


Figure 3-10. Configure media port ranges

You can set up a port range using PowerShell as well.

2. Configure a separate GPO for each modality.

After defining port ranges in the Teams admin center, you must create QoS policies that specify the DSCP values to be associated with each port range. Basically, restricting a set of ports to a specific type of traffic does not result in packets traveling through those ports being marked with the appropriate DSCP value. In addition to defining port ranges, you must also create QoS policies that specify the DSCP value to be associated with each port range. This DSCP value's association with a port range can be achieved via GPO, which is called policy-based QoS. With QoS policy, you

can configure and enforce QoS policies that cannot be configured on routers and switches [99a]. QoS policy provides the following advantages:

- QoS policies are easier to configure by using a user-level QoS policy on a domain controller and propagating the policy to the user's computer.
- QoS policies are flexible. Regardless of where or how a computer connects to the network, QoS policy is applied. The computer can connect using Wi-Fi or Ethernet from any location.
- Some QoS functions, such as throttling, are better performed when they are closer to the source. QoS policy moves such QoS functions closest to the source.

If you already have all port ranges and DSCP values with media category type, then proceed to the next step. If not, then decide on port ranges and follow Step 2 for configuring port ranges.

Microsoft outlines the complete steps and port ranges at <https://docs.microsoft.com/en-us/microsoftteams/qos-in-teams>.

- a. You must have consolidated all your computer objects to single OU. For example, the Bloguc Organization consolidated all computers under the PC OU to apply GPO correctly. You can apply a single GPO to multiple OUs; however, for better management, consolidate objects into one OU and then apply the policy.
- b. Log in to the domain controller or computer that has Group Policy Management installed.

- c. Open the Group Policy Management tool (Run ► gpmc.msc) and then right-click the OU (Computer). Click Create A GPO In This Domain And Link It Here to create a new GPO; for example, TeamsClient-QoS. You must have the required permission (domain admin or the like) to create and link policy object permission.
- d. Select the newly created GPO and right-click it. Select Edit to Open Group Policy Management Editor. Expand Computer Configuration ► Policies ► Windows Settings. Right-click Policy-based QoS, then select Create New Policy, as shown in Figure 3-11.

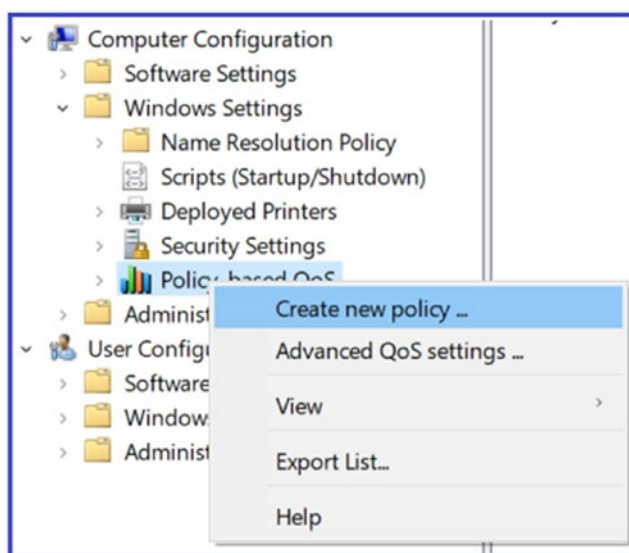


Figure 3-11. Policy-based QoS

- e. On the Policy-based QoS page, shown in Figure 3-12, give the policy a name, such as Teams Audio. Select the Specify DSCP Value check box and enter the value 46. Click Next.

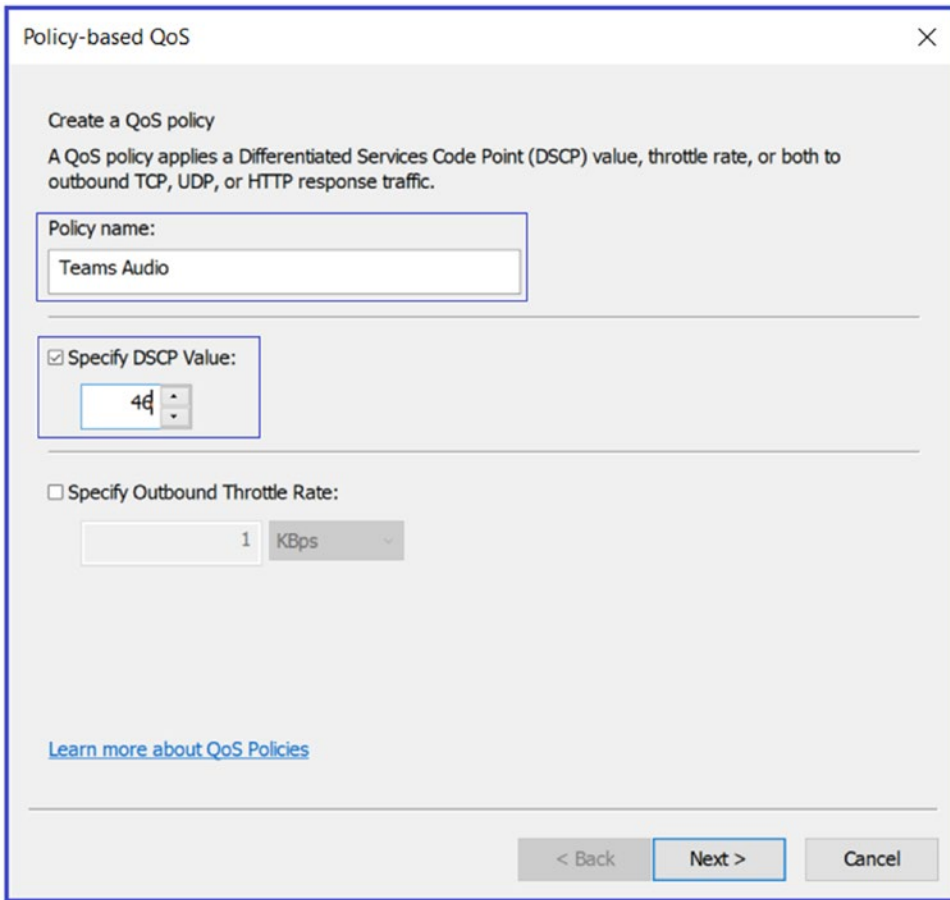


Figure 3-12. *Specifying the policy name and DSCP Values*

- f. On the next page, shown in Figure 3-13, select the Only Applications With This Executable Name option, and enter Teams.exe. Click Next.

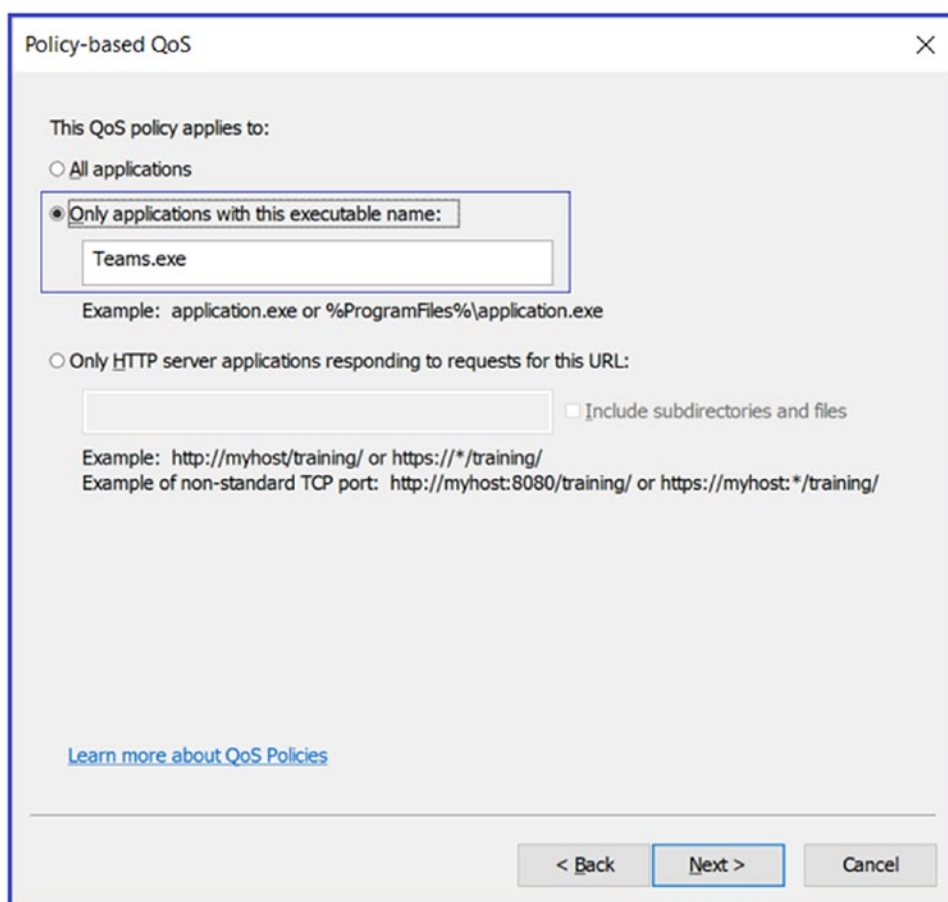


Figure 3-13. Application name

Note This simply ensures that the Teams.exe application will match packets from the specified port range with the specified DSCP code.

- g. On the next page, make sure that both the Any Source IP Address and Any Destination IP Address options are selected, as shown in Figure 3-14. Click Next.
-

Note These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.

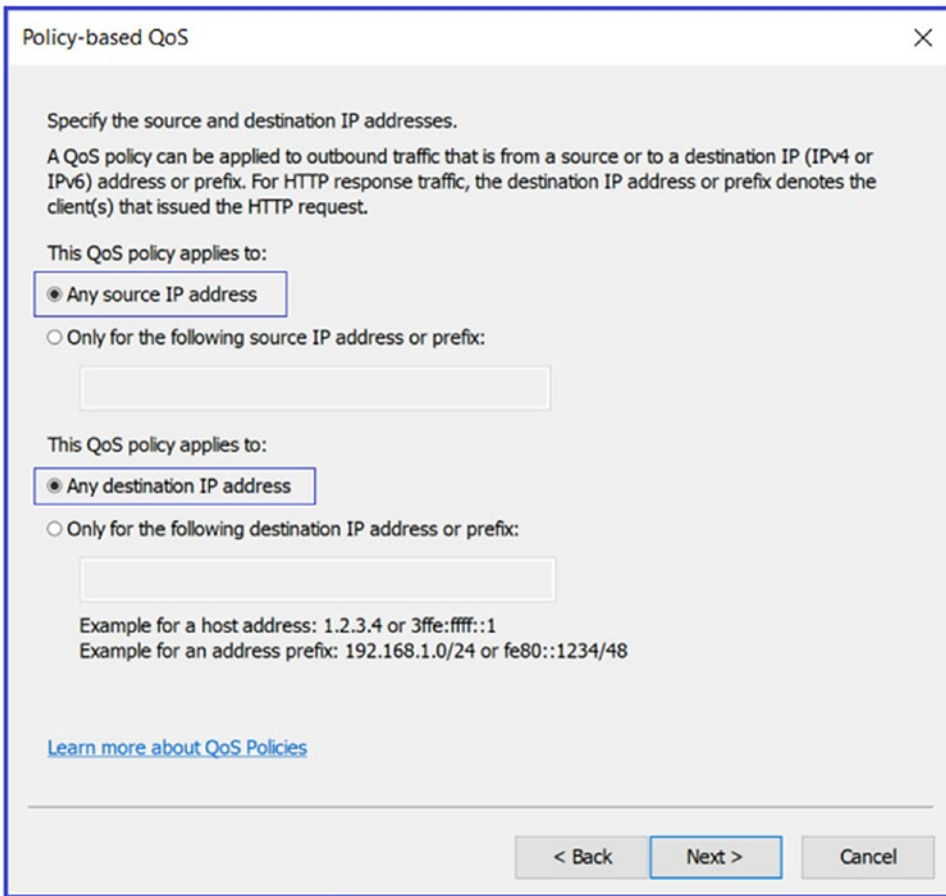


Figure 3-14. *Selecting the IP addresses that the QoS policy applies to*

- h. On the next page, for the Select the Protocol This QoS Policy Applies To setting, select TCP and UDP. Select From This Source Port Number Or Range. Also, enter a port range reserved for audio transmissions (50000–50019) and select To Any Destination Port. Figure 3-15 shows protocol and port range configuration information.

Note Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the two networking protocols most commonly used by Microsoft Teams Service and its client applications.

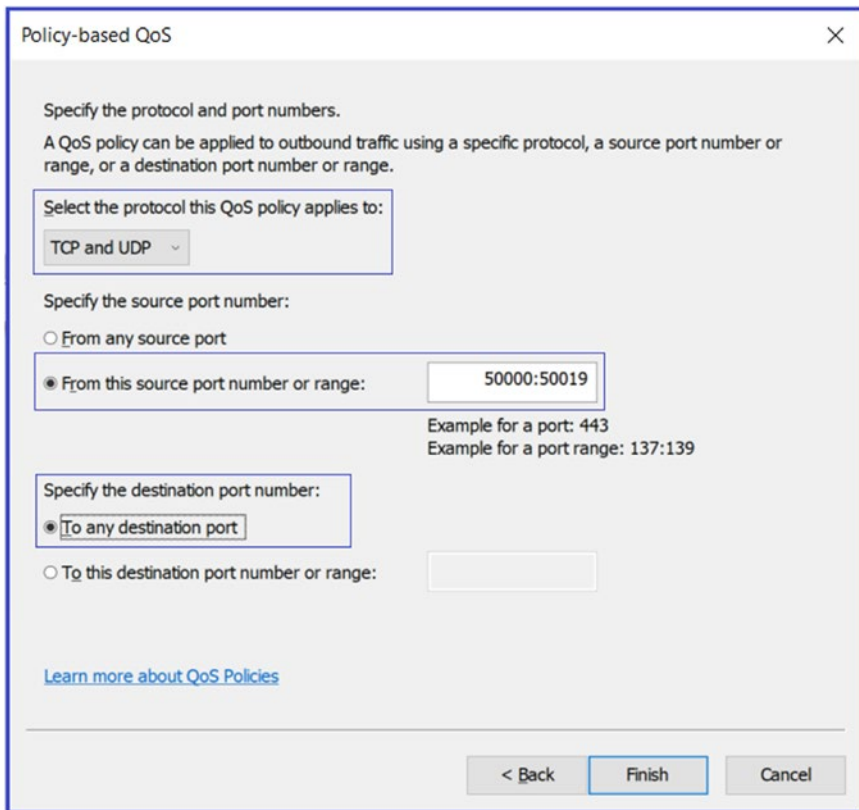


Figure 3-15. Defining source port number or range

- i. Follow Steps e to h and create new policy objects as Teams Video and Teams Sharing with the given port ranges and DSCP values.
- j. After you are finished configuring all policy objects, it will look like Figure 3-16.

Policy Name	Application	Name o...	Protocol	Source Port	Destination ...	Source IP / P...	Destination ...	DSCP Value
Teams Audio	Teams.exe		TCP and UDP	50000:50019	*	*	*	46
Teams Video	Teams.exe		TCP and UDP	50020:50039	*	*	*	34
Teams Sharing	Teams.exe		TCP and UDP	50040:50059	*	*	*	18

Figure 3-16. All policies

- 3. Finally, test the QoS. As a best practice, you must validate QoS configuration and DSCP tagging on a quarterly basis.

Verifying QoS Policies Are Applied

After QoS policy configuration, you must verify all QoS settings. There are multiple ways to verify the QoS.

- *Using Registry on Windows local computer:* Once the GPO pushed and applied to the computer, you can force the GPO to the local computer by running the command `gpupdate.exe /force`. Then visit the Registry path `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\QoS\Teams Audio` to verify that QoS policies have been applied. Figure 3-17 shows Teams Audio, Teams Video, and Teams Sharing policies with port ranges and DSCP values.

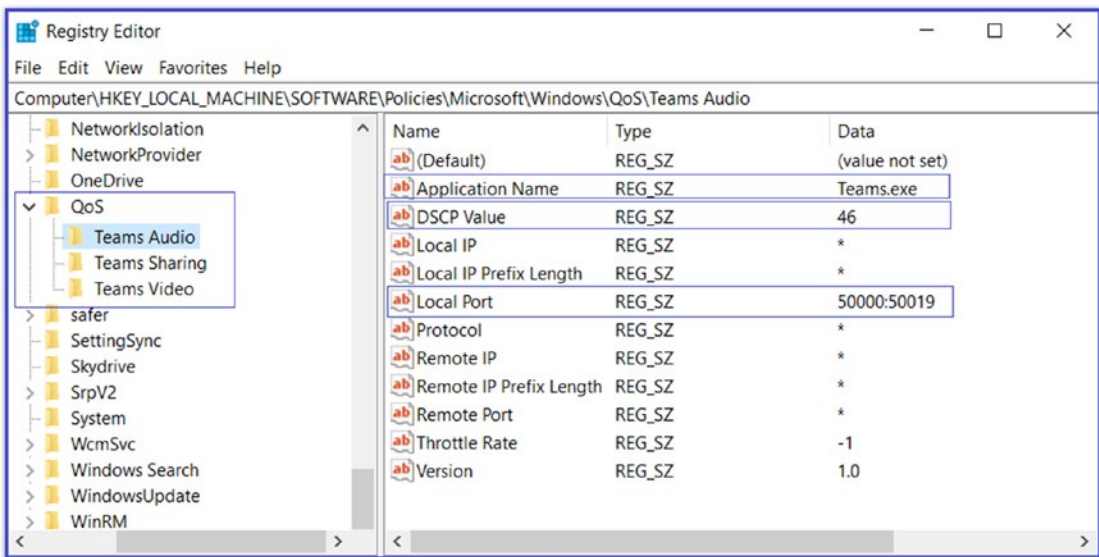


Figure 3-17. Verifying QoS using local computer registry

- *Validate QoS tagging using packet capture:* You need Wireshark as a network packet capturing tool. Start a Teams audio/video meeting and capture the network traffic via the Wireshark tool (it is a freeware tool that you can download and install on your computer). Figure 3-18 shows Teams audio traffic (the source is 10.0.0.207 and destination is 104.42.192.49) protocol UDP with the port number 50018. This packet shows DSCP marked as EF (expedite forwarding as DSCP 46). Verify the two-way traffic to get QoS benefits.

4554	65.947508	10.0.0.207	104.42.192.49	UDP	85 50018	→ 51410	Len=43
4555	65.947839	10.0.0.207	104.42.192.49	UDP	957 50018	→ 51410	Len=915

```

Frame 4555: 957 bytes on wire (7656 bits), 957 bytes captured (7656 bits)
Ethernet II, Src: IntelCor_44:64:d9 (00:28:f8:44:64:d9), Dst: ArrisGro_e6:23:1e (5c:b0:66:e6:23:1e)
Internet Protocol Version 4, Src: 10.0.0.207 (10.0.0.207), Dst: 104.42.192.49 (104.42.192.49)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  Total Length: 943

```

Figure 3-18. Validating QoS tagging

Deploying VPN Split Tunnel for Microsoft Teams Media Traffic

It's common for an organization to use remote access or a VPN solution that offers an encryption tunnel between endpoints, like remote users and the corporate network. Usually, VPNs are not designed to support real-time media traffic and introduce an extra layer of encryption on top of Teams media traffic that is already encrypted. This means it adds overhead to Teams media packets. Additionally, connectivity to the Teams service (Office 365) might not be efficient due to hair-pinning traffic through a VPN device. For VPNs, the suggestion is to provide an alternate path that bypasses the VPN tunnel for Teams traffic. This is generally known as split-tunnel VPN.

Understanding Split-Tunnel VPN for Teams Media Traffic

Because there are multiple VPN solutions available in the market and every solution vendor might have a different process to implement split-tunnel VPN, this topic covers general recommendations as to what should be configured on the VPN solutions. There are multiple rationales for which you, as a Teams admin, must implement split-tunnel VPN.

- For Microsoft Teams conversation and collaboration features, VPN or remote access connections are usually acceptable because the network qualities were frequently not visible to the end user. If a chat message arrived a second or two later, there would be only a minor impact. The same is not applicable for keeping a bidirectional conversation in real time, like a Teams audio call.

- Microsoft Teams uses a number of codecs, and they have different packetization times. However, VPN solutions add another layer of encryption and decryption, which greatly increases network latency on these packets getting to their destination in a timely manner. When these Teams media packets are delayed or received out of order, jitter increases and the receiving endpoint will attempt to fill in and stretch the audio to fill in the gaps, which usually results in undesired audio effects like robotic noise, voice speed up, and so on.
- A VPN solution contributes to intermittent difficulties like random network disconnections, which will cause the Microsoft Teams session to disconnect (disruption of the signaling path) or media quality issues. This would generally indicate a need for increased capacity on the VPN solution. However, when the VPN solution was designed, this likely wasn't factored in, and the media usage is degrading the overall VPN experience for other applications as well.
- Clients who have configured their VPN solution to exclude Microsoft Teams traffic or implement split-tunnel VPN have seen great returns in user satisfaction not specific to the Teams audio and video experience. For this purpose, we strongly recommend leveraging the steps that follow to complete a split-tunnel VPN for Teams media traffic over VPN solutions.

Split-Tunnel VPN Architecture

Providing optimal call quality to the end user who uses Teams over VPN requires a split-tunnel VPN solution. In a split-tunnel VPN configuration, all IP addresses that are used by the Microsoft Teams services (Office 365) environment are excluded, so that traffic to and from those IP addresses is not included in the VPN tunnel. This means the split-tunnel VPN must work exactly the same way as the external Teams client should. Most VPN solution providers support split-tunnel VPN; you must check the configuration for your VPN solution by checking vendor documentation. Figure 3-19 shows how split-tunnel VPN works [14b].

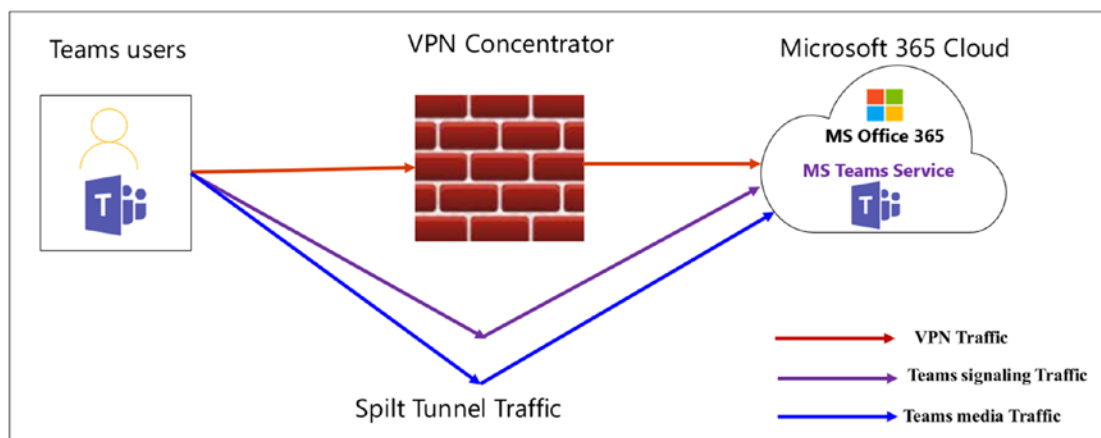


Figure 3-19. Split-tunnel VPN traffic flow

All Microsoft Teams signaling and media traffic split from the VPN secure tunnel, as shown in Figure 3-19, and go through Microsoft Teams service (Office 365). To redirect users away from the VPN solution for Teams, it must first be configured to support a split tunnel, which is a popular feature of today's VPN appliances. Split-tunnel VPN allows Teams traffic without going through the VPN tunnel. For example, the external web traffic from the Teams site teams.microsoft.com does not traverse over the VPN solution. Without split tunnel, the default VPN configuration will force all the Teams traffic through the VPN tunnel.

Implementing Split-Tunnel VPN

There might be different way to achieve a VPN split tunnel for Teams media and signaling traffic, such as using a firewall or third-party VPN solution. I have mentioned here one of the ways that is commonly used to configure VPN split tunneling using a third-party VPN.

Using a Third-Party VPN Solution

In this topic, we cover split-tunnel VPN configuration based on the Pulse secure VPN solution as an example. I strongly recommend contacting your VPN vendor for split-tunnel configuration documentation. There are different approaches and solutions to implement split-tunnel VPN, and I present here a combined solution to use a VPN concentrator and your corporate firewall.

We are creating a policy on a VPN concentrator to exclude Microsoft Teams service IP addresses (Office 365) traffic from the VPN tunnel. This means denying signaling and media traffic via the VPN tunnel for Teams service IP addresses (Office 365). Then, using your corporate firewall, create a deny rule to deny traffic sourced from the VPN user subnet to Teams service IP addresses (Office 365) and from Teams service IP addresses (Office 365) to VPN user subnets both ways.

The split-tunnel solution is a combined solution using a VPN concentrator and your firewall.

1. First, get all Teams service IP addresses, including optimized required and allow required. Refer to the Microsoft documentation for Teams service IP addresses at <https://docs.microsoft.com/en-us/Office365/Enterprise/urls-and-ip-address-ranges>.
2. Create a policy on a VPN concentrator, which will exclude traffic via VPN tunnel for all Teams service IP addresses (refer to the preceding URL for Teams IP addresses). In other words, deny traffic or split tunnel to these Teams IP addresses from your VPN tunnel and assign this policy to all other policies and users.
3. Now work with your network firewall team and do this. Split Teams conferencing (media) traffic to external (not via VPN tunnel).

Remember, all-conference modality traffic is involved through a multicontrol unit (MCU) running on Teams service (Office 365). First, create the following firewall rules.

- Create a firewall rule that will block traffic going from VPN user subnets to Teams service IP addresses or subnets (Office 365). Refer to the earlier Microsoft documentation link.
- Create another firewall rule that will block traffic going from Teams service IP addresses or subnets (Office 365) to the VPN user subnet.

To implement split-tunnel VPN for Teams one-to-one call traffic, you must create more rules on your corporate firewall.

Apart from the Teams conferencing traffic, you can enable the blockage of the UDP/TCP source port for Teams audio, video, and application sharing. Basically, Microsoft Teams, by default, has a limited scope of UDP/TCP ports it will be using as the source

ports for communication. If you block these source ports from entering the VPN tunnel, then the media should go via the external split from the VPN tunnel. That will ensure even two users both connected via VPN, and their Teams media traffic, will not allow hair-pinning via their VPN connection, but goes directly from one Internet connection to the other.

The sample firewall rules look like this:

- Create a firewall rule source address from the VPN_Users subnet to the destination as Any with the application Stun and Teams (if allowed) and Service port (UDP/TCP port ranges of audio, video, and application sharing).
- Create another firewall rule source from any address to the destination VPN_Users subnet with the application Stun and Teams (if allowed) and Service port (UDP/TCP port ranges of audio, video, and application sharing).

You can get Teams audio/video and application sharing client port ranges from the Teams admin center. Log in to the Teams admin center, then go to a meeting. In Meeting Settings, under Network, select Get New Image.

DOES THIS TOPIC APPLY TO SKYPE FOR BUSINESS ONLINE?

Yes, this topic is applicable to Skype for Business Online as well, because Microsoft Teams and Skype for Business Online share the same IP subnets and ports.

Verifying VPN Split Tunneling

To verify the VPN split tunnel, you must connect using the external network (wired or wireless) and then connect the VPN, which has the split tunnel implemented.

1. Make a Teams one-to-one call and capture network traces using Wireshark or Network Monitor and verify Teams media (UDP) traffic going between your local IP and other party local IP addresses (not via VPN IP addresses).

2. Join the Teams meeting, and capture network traces using Wireshark or Network Monitor and verify Teams media (UDP) traffic going between your local IP address and Teams service IP address (Office 365) transport relay and not via VPN IP addresses.

Note For the Teams service IP addresses or subnet block rule on the firewall, set the action as Reset instead of denying. That allows for a faster Teams client sign-in.

Providing optimal experience to the end-user community is our main goal, and using VPN split tunneling helps to achieve this through blocking the Teams client from connecting via VPN tunnel. The media will then always go through externally, not via VPN tunnel, which will eliminate extra hops, double encryption, and so on.

Summary

In this chapter, you learned detailed information about network assessment and bandwidth planning for Teams, how to deploy and manage QoS, and how to deploy split-tunnel VPN for Microsoft Teams media traffic. Before the deployment of Microsoft Teams in a production environment, you, as an admin, need to evaluate if the existing network meets the networking requirements of Microsoft Teams. Make sure that you have the required bandwidth, access to all required IP addresses, the correct ports opened, and that you are meeting the performance requirements for Teams real-time media traffic such as audio, video, and application sharing.

CHAPTER 4

Teams Audio Conferencing and Phone System Management

Microsoft Teams provides different capabilities, such as persistent chat, audio and video calls, conferences (dial-in and client join), and phone systems (inbound/outbound PSTN calls). So far you have learned how Teams features work, their interaction with other components, and management aspects. This chapter covers Teams conference management including audio conferencing (dial-in) and VoIP for both internal and external attendees and Teams Phone System management including Teams Direct Routing, Calling Plan, and voice routing policies.

After this chapter, you will be able to understand and manage the following tasks.

- Plan and manage Teams conferences.
- Teams Audio Conferencing includes Teams service and phone numbers, Teams meeting settings, default conference number and language management, Conference ID and PIN number management, and the ability to customize and configure Teams meetings invitations.
- Teams Phone System planning.
 - Configuring and managing Teams Direct Routing.
 - Configuring and managing Microsoft Calling Plan.
 - Configuring and managing Call Queue.

- Configuring and managing Teams emergency service.
- Managing phone number and voice routing policy.
- Voice routing policy (dial plan, voice routing policy, and PSTN usages).

Planning and Managing Teams Conferences

Microsoft Teams Conferences

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

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

Teams also provides an extra layer of engagement before, during, and after meetings. For example, before a meeting you can have a background conversation in Teams and prepare and discuss content, then schedule a Teams meeting. Throughout a meeting you can use face-to-face video, you can follow the action, you can share content, you can record the meeting with transcription and easily join from a Teams room. After a meeting you can play back the meeting with transcription, you can share notes, and have a postmeeting chat for collaboration. This makes Teams meetings uniquely reliable, reduce quality complaints drastically.

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

Organizing Teams Meetings Efficiently

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

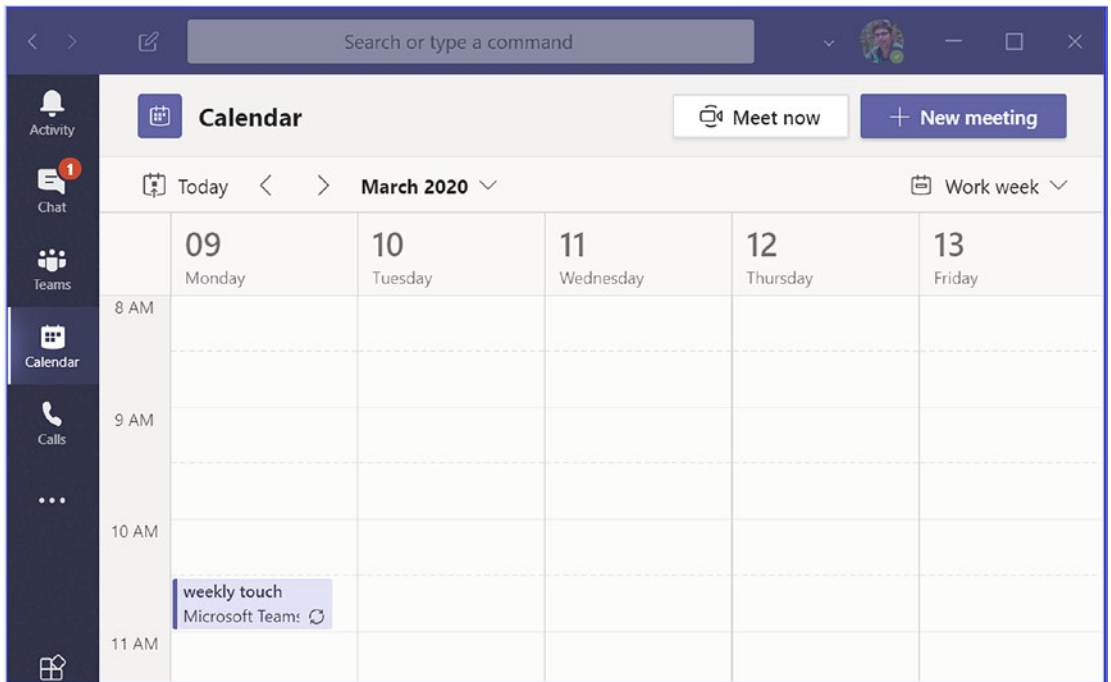


Figure 4-1. Calendar daily and weekly view

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

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

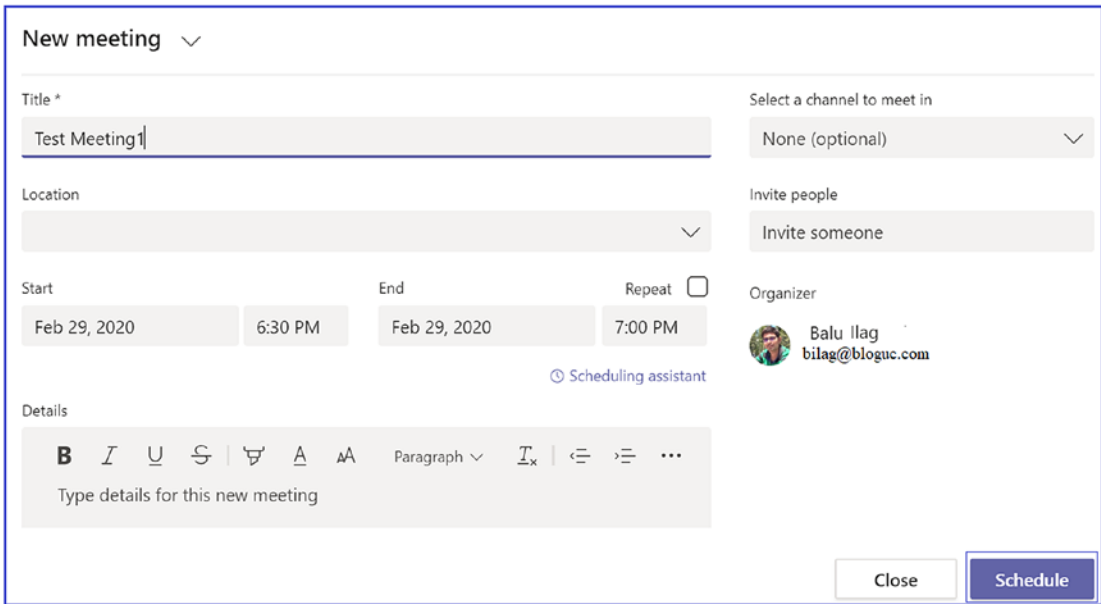


Figure 4-2. *Setting up a new meeting*

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

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

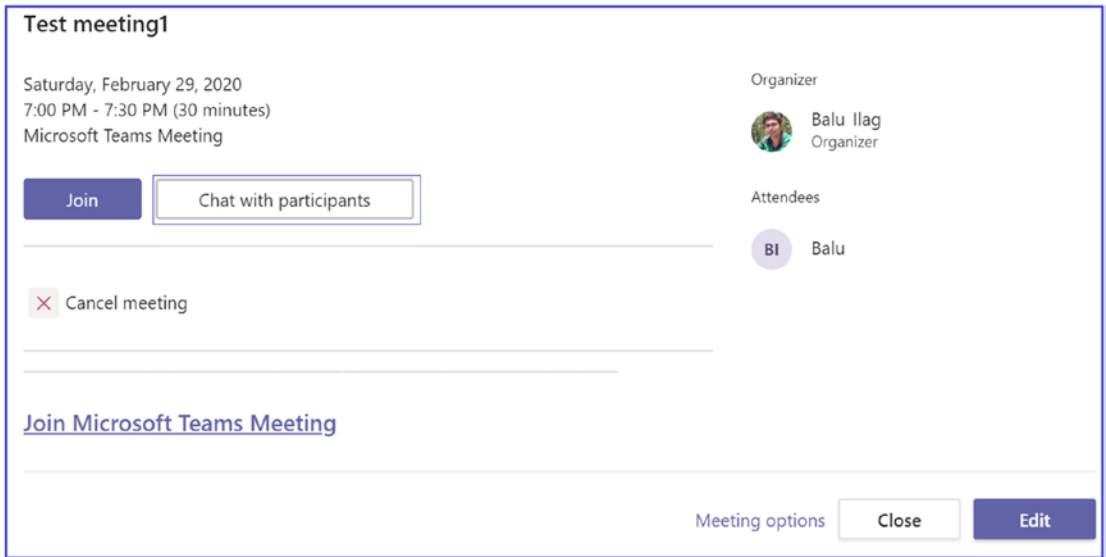


Figure 4-3. *Chat With Participants option*

Figure 4-3 shows that the premeeting chat looks just like a regular Teams conversation. Not only can you have conversation here, but you can also share any file, upload a PowerPoint presentation, or ask for opinions on the presentation.

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

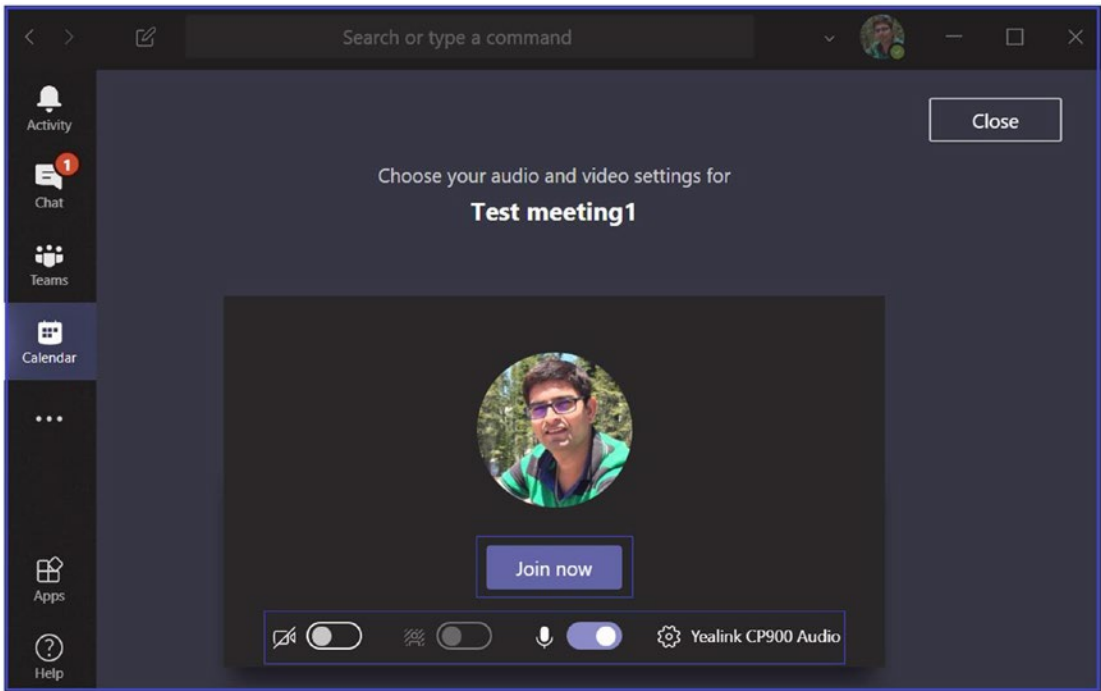


Figure 4-4. *Joining a meeting*

Once you are ready to join the meeting, click Join to enter the meeting. Once you are in the meeting, there are a number of controls that you can use, including turning your camera on or off, mute or unmuting your microphone, sharing a presentation and desktop, and other things. In the upper right corner, other items manage participants and access chat. Figure 4-5 shows these meeting controls.

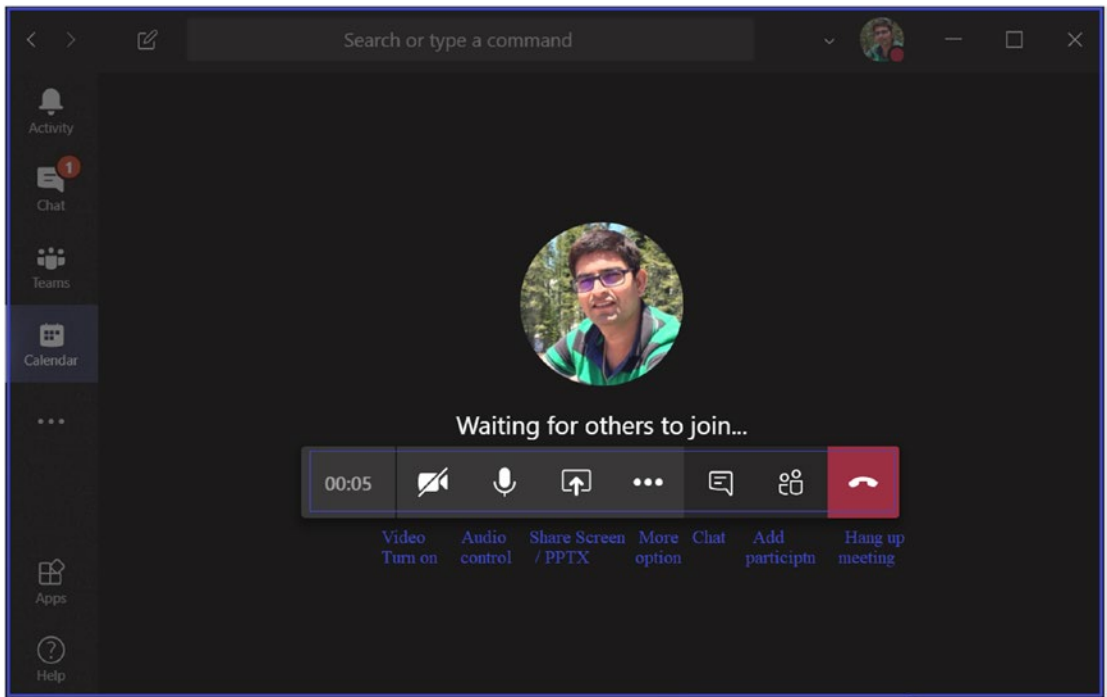


Figure 4-5. Meeting controls

During the meeting, you will be able to see user-shared PowerPoint presentations that might be discussed during the meeting. Also, on the right side you can see the chat display.

The postmeeting experience can include a meeting recording, presentation files shared during the meeting, and all discussion that happened during the meeting. The recording is available for everyone who was a part of the calls, and they can view the recording in Teams (recording is only available if the meeting was recorded).

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

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

Teams Meeting Attendee Types

Teams meetings have different attendee types. Depending on what type of attendee you are, you will have different information and options available to use during meetings.

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

Remember, that attendee type is determined at join time and you cannot change that. For example, if a federated user forgets to sign in, he or she will be treated as an anonymous user when joining Teams meetings. If that user wants to join a meeting as a federated user, then he or she must leave the meeting and rejoin as a federated user by signing in is possible to promote attendees from one attendee type to a different type, such as attendee to presenter in meeting.

Meeting Attendees' Experience

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

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

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

Which Teams Clients Can Join a Meeting?

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

- *From desktop client:* You can use a Windows or Mac client, or you can use a web client (Edge, Chrome, or Safari).
- *From mobile:* You can use an Android or iOS Teams app to join a Teams meeting.
- *From a desktop phone:* You can use 3rd Party IP Phone (3PIP) phones and phones optimized for Teams.
- *From a PSTN phone:* You can do dial in to or dial out from a Teams meeting.
- *From a room system:* You can join a Teams meeting using Skype Room System v2, Teams room or Surface Hub.
- *Cloud video interop:* You can use third-party solutions to integrate with existing room systems.

Teams Licensing for Meetings

Regarding licensing, Teams meetings are included in almost all the Teams licenses, with the exception of the F1 license, which does not have Teams meetings (the F1 license does allow one-to-one calls and joining meetings, but does not allow users to create meetings). If you want to use Teams Audio Conferencing, which gives the ability to dial in and dial out from and to phones, this requires an additional license. Audio Conferencing is included in the E5 license or is available as an add-on for E1 and E3 licenses.

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

Teams Meeting Delegation

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

Recording with Microsoft Stream

To record a Teams meeting, users must have an E1, E3, E5, A1, A3, A5, M365 Business, Business Premium, or Business Essentials license assigned with a Microsoft Streams license. Additionally, users must have Stream upload video permission. If there is any consent set by an admin, then it must be accepted and enough storage must be available in Stream for the recording to be saved.

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

Microsoft Teams Meeting Networking Considerations

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

Where Teams Meetings Are Hosted

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

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

Networking Considerations for Teams Meeting Deployment

You already know that Teams is a cloud-only service, which means the Teams client is registered against a Teams service in the cloud and Teams meeting attendees have to join the meeting through Teams service in cloud. Therefore all Teams signaling and

media traffic traverses through the corporate network to the Internet to the Microsoft cloud network. That’s why your Teams meeting planning for networking must include these three network segments, as shown in Figure 4-6.

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

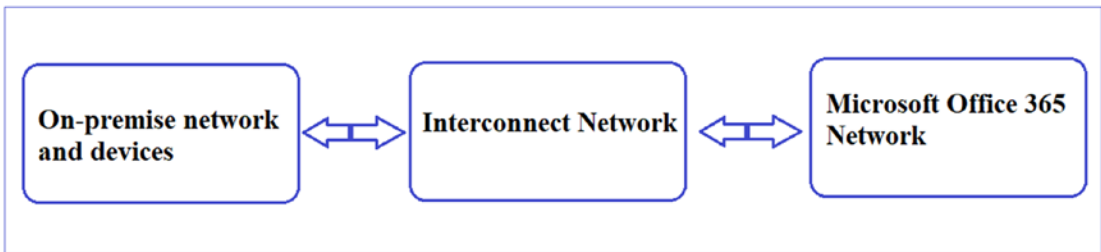


Figure 4-6. Teams traffic traversing across the networks

Allowing Teams Inbound and Outbound Traffic Through Firewall Configuration

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

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

It is recommended that you bypass Teams traffic from any packet inspection or security stack that might add latency or hold the packet for inspection.

Managing a Teams Meeting

Meeting Configuration

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

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

Meeting Settings Applied to All Meetings

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

Meeting Policies Assigned to Users

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

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

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

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

Creating and Managing Meeting Policy

You can create new meeting policy or manage existing meeting policy using the Teams admin center. To create a new meeting policy, follow the steps given next. In a meeting policy, there are four sections: General, Audio & Video, Content Sharing, and Participants & Guests.

1. Log in to the Teams admin center. In the left navigation pane, select Meetings. Select Meeting Policies. Click + Add to create a new meeting policy.
2. Once the New Meeting Policy Page opens, then enter a meaningful name for the new policy, and optionally enter a description. In the General section, select whether to turn the following options on or off:
 - *Allow Meet Now In Channels*: This option allows users to host a meeting in the team channel.
 - *Allow the Outlook Add-in*: This option is important because users can schedule Teams meetings through Outlook.
 - *Allow Channel Meeting Scheduling*: This feature allows users to schedule channel meetings.

- *Allow Scheduling Private Meetings:* -This feature allows users to schedule private meetings.

Figure 4-7 shows all options in the General section set to On.

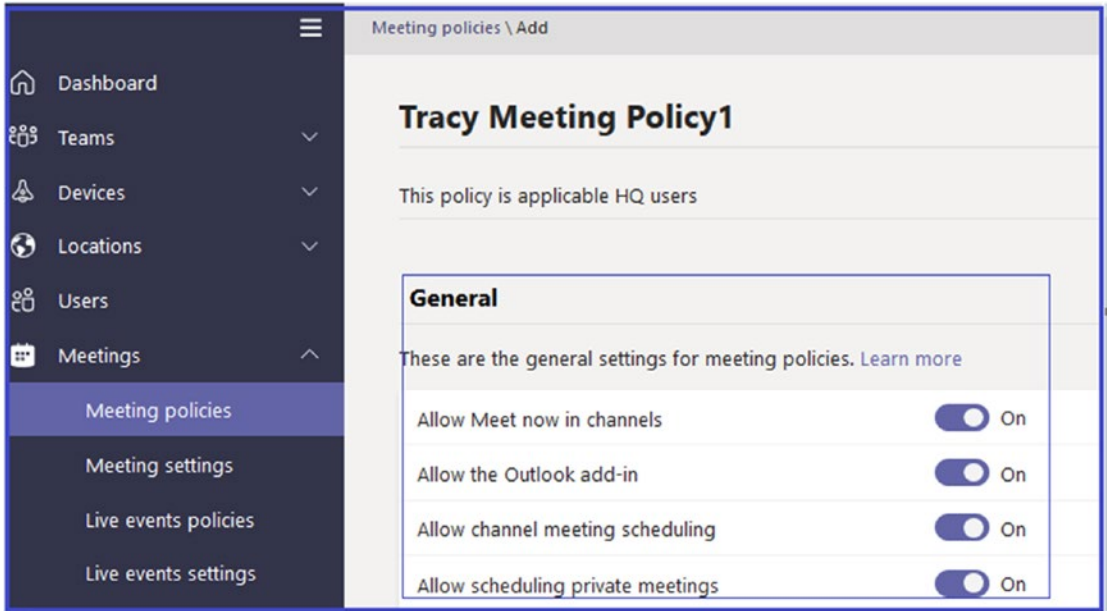


Figure 4-7. Meeting policy general settings

For example, Allow Meet Now is a policy 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 feature on, when a user posts a message in a Teams channel, the user can select Meet Now to initialize an ad-hoc meeting in the channel.

3. In the Audio & Video section, turn the following options on or off.
 - *Allow Transcription:* You can turn on or off transcription for a meeting.
 - *Allow Cloud Recording:* This is a popular feature among users.
 - *Allow IP Video:* When this setting is enabled, you can also enter the media bit rate in KBs, which determines the media bit rate for audio, video, and video-based app sharing in meetings.

Figure 4-8 shows a summary of the Audio & Video settings.

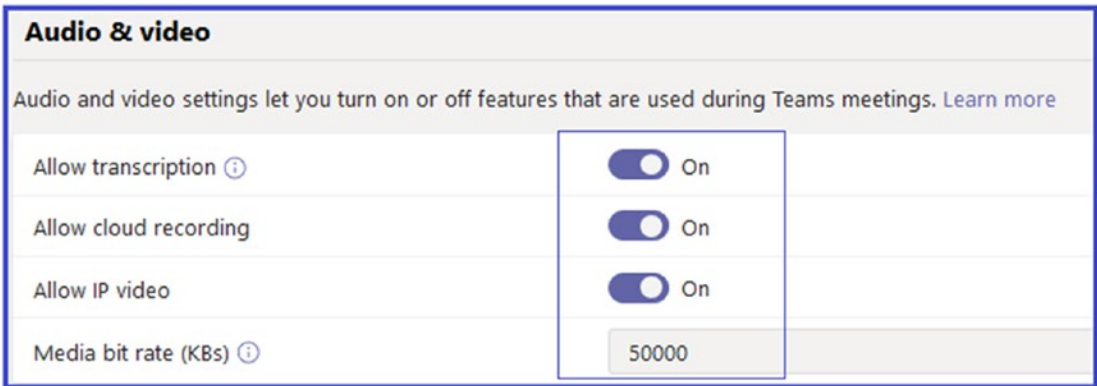


Figure 4-8. *Audio & video settings*

For example, if the Allow Cloud Recording setting is enabled and the user is authenticated as a user from the same organization, then the recording can be started by the meeting organizer or another meeting participant. This only applies to the internal users; guest users do not have permission to start or stop the recording.

4. In the Content Sharing section, shown in Figure 4-9, first select one of the Screen sharing modes: Entire Screen, Single Application, or Disabled. Then turn the following options on or off.
 - Allow A Participant To Give Or Request Control
 - Allow An External Participant To Give Or Request Control
 - Allow PowerPoint Sharing
 - Allow Whiteboard
 - Allow Shared Notes

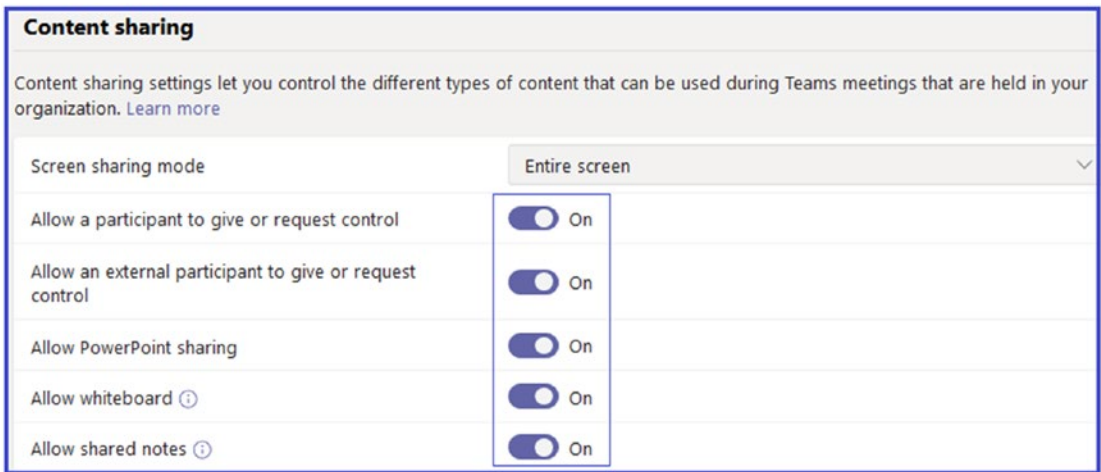


Figure 4-9. Content Sharing settings

For example, the Allow A Participant To Give Or Request Control setting defines whether the user can give control of the shared desktop or window to other participants who are present in the meeting.

5. In the Participants & Guests section, you can select to turn these options on or off.
 - Let Anonymous People Start A Meeting
 - Allow Dial-In Users To Bypass The Lobby
 - Allow Meet Now In Private Meetings

Then select the other feature options listed here.

- Automatically Admit People: Select one of the following options:
 - a. Everyone
 - b. Everyone In Your Organization
 - c. Everyone In Your Organization And Federated Organizations
- *Enable Live Captions*: Select one of the following options.
 - a. Disabled But The Organizer Can Override
 - b. Disabled

- *Allow Chat In Meetings:* Select one of the following options.
 - a. Enabled
 - b. Disabled

Once you have finished entering your settings, click Save to commit the changes. Figure 4-10 which shows the recommended feature selections.

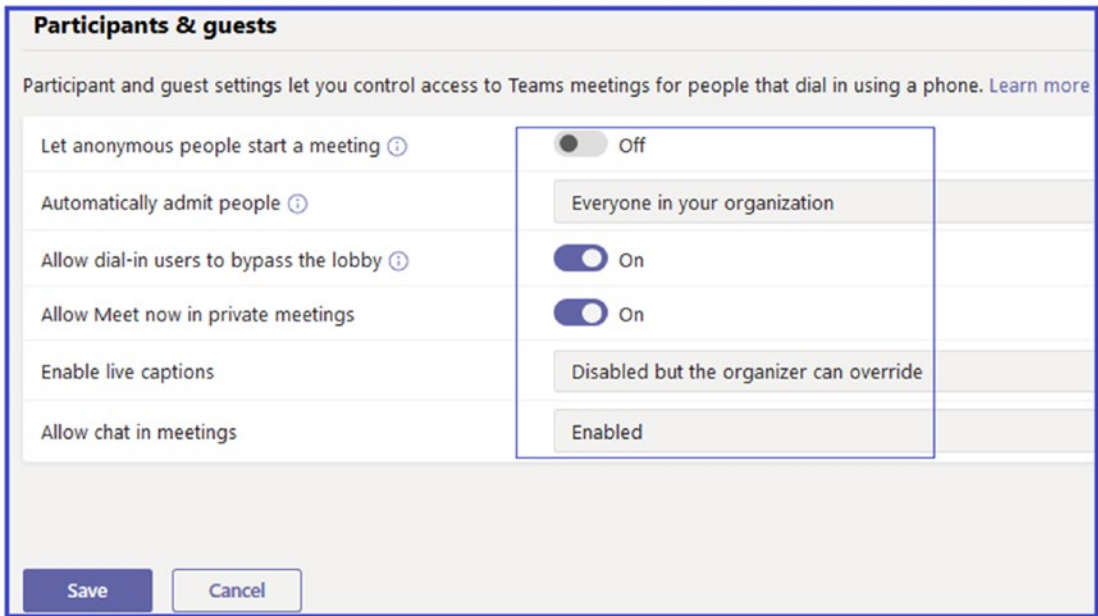


Figure 4-10. Participant & Guest settings

As another example, if you turn off Allow Channel Meeting Scheduling, then the Schedule A Meeting option will not be available to users when they start a meeting in a Teams channel, and the Select A Channel To Meet option will not be available to the users when they schedule a meeting in Teams.

Checking Teams Meeting Quality

To check the quality of Teams meetings, there are two tools you can use. The first is CQD, which gives aggregated views of call quality and can be used to investigate quality per building, per subnet, or any other metric that makes sense in your scenarios. You can use CQD to proactively identify quality issues by looking at the lowest quality site

and determining how you can improve call quality. To access CQD, log in to the Teams admin center and then click Call Quality Dashboard. You might need to sign in again in to CQD.

Call analytics is the second tool you can use. This allows you to view individual calls and see what the quality for a certain call was, for both one-to-one calls and Teams meetings. Call analytics can be used reactively to troubleshoot individual calls that a user reports as a poor call quality experience. To access call analytics, log in to Teams admin center and then select Users. Find the individual user whose call quality you want to check and then click Call History. Select the individual call to check call quality, as shown in Figure 4-11.

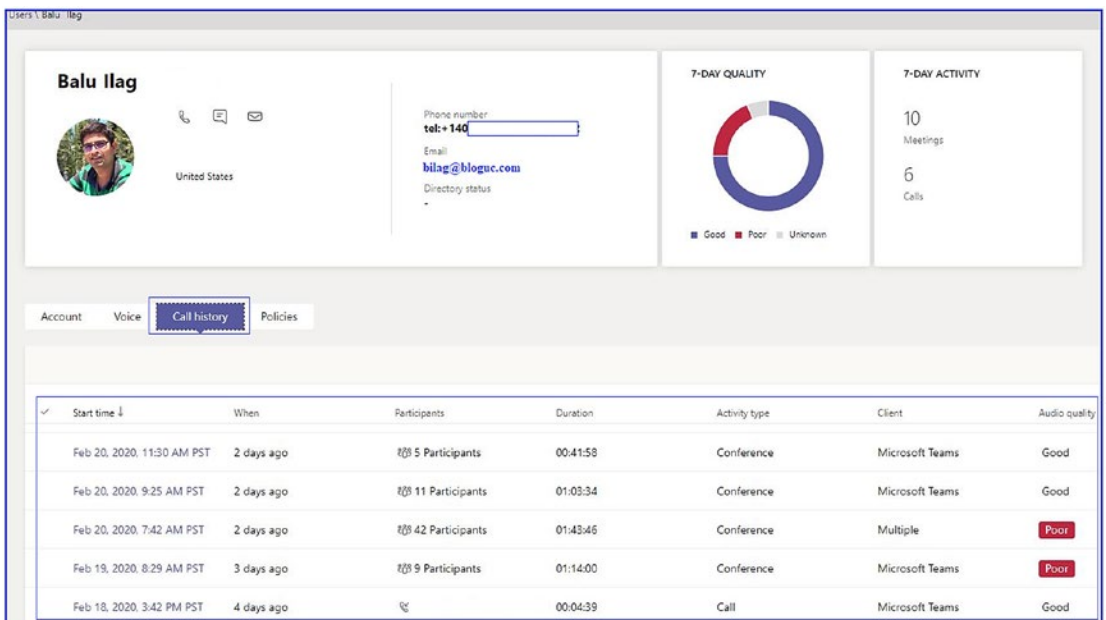


Figure 4-11. Call analytics

Microsoft Teams Audio Conferencing

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

This topic covers Teams Audio Conferencing (dial-in), including how Teams Audio Conferencing works, how to acquire a conference bridge, Audio Conferencing licensing, dial-out limits, and more. Teams Audio Conferencing allows attendees to join Teams

meetings through dial-in to a Teams conference bridge number with a conference ID through a regular phone (landline or mobile phone). Teams Audio Conferencing is also known as Teams dial-in conferencing. For example, using Audio Conferencing, users can attend meetings over a regular phone by dialing in to the meeting.

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

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

Before deploying Teams Audio Conferencing across your organization, you should ensure that all user locations have Internet access to connect to Office 365 (Internet breakout for each branch and central site is ideal). If it is not possible to have direct Internet connectivity for each branch site, at least check network quality using the Network Testing Companion tool that shows network quality, including packet loss, jitter, and latency. You will therefore have an idea what experience users are going to have when they use Teams meetings. Additionally, you must check whether your network is ready for a deployment of Microsoft Teams meetings. Before learning about Teams Audio Conferencing, as a Teams admin you must know what type of phone numbers Teams supports.

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

Teams Audio Conferencing Licensing Requirements

To use Teams Audio Conferencing, your organization needs an additional license on top of the Microsoft Teams license. Microsoft 365 Audio Conferencing (Teams Audio Conferencing) licenses are available as part of an Office 365 E5 subscription or as an add-on license to an existing subscription like E1 or E3.

Teams Audio Conferencing Requirements

Teams Audio Conferencing involves the Audio Conferencing licenses, the conference dial-in bridge (phone numbers for dial-in), and Communications Credits for dialing out from Teams meetings. As part of the Teams Audio Conferencing license, Microsoft provides dedicated dial-in bridge numbers (an admin must acquire the dial-in numbers from Microsoft) and shared conference numbers. If your organization is using a legacy solution like Skype for Business (Lync) On-Premises or Online with enterprise voice and dial-in conferencing with their own conference bridge numbers, then the organization might want to use the existing conference bridge for Teams meetings when upgrading from Skype for Business to Microsoft Teams. As of this writing, Microsoft does not support moving to or using existing or on-premises conference bridge numbers for Teams Audio Conferencing dial-in numbers. This means you must use Microsoft-provided conference bridge numbers either dedicated or shared.

As a Teams admin, you must understand how to configure a Teams conference bridge number. Conferencing bridge numbers allows users to dial into meetings through a landline or mobile phone. When configuring Teams Audio Conferencing in your Office 365 environment, you will receive conference bridge numbers from Microsoft for what is called an Audio Conferencing bridge (a conferencing bridge can contain one or more phone numbers). These conference bridge numbers are used when the users dial in to a Teams meeting (the phone number should be included in every Microsoft Teams meeting invite). Shared audio conference bridge number automatically assigned to the organization tenant when it enables (assigned the audio conference license) for audio conference. However, a dedicated conference bridge number (ToLL or Toll-free) available based on request. As an admin, you can acquire a Toll or Toll-free number from Microsoft using the Teams admin center or sending an email to the Microsoft service desk to obtain a conference number.

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

Adding Additional Dedicated Conference Bridge Numbers

To add a dedicated conference bridge number, you must perform the following steps.

1. Log in into the Teams admin center and in left pane, select Meetings. Then select Conference Bridges. On the Conference Bridges page, click + Add.
2. From the + Add drop-down list, select either Toll Number or Toll-Free Number, as shown in Figure 4-12.
3. On the Add Phone Number Page, select the phone number you want to add, and then click Apply.

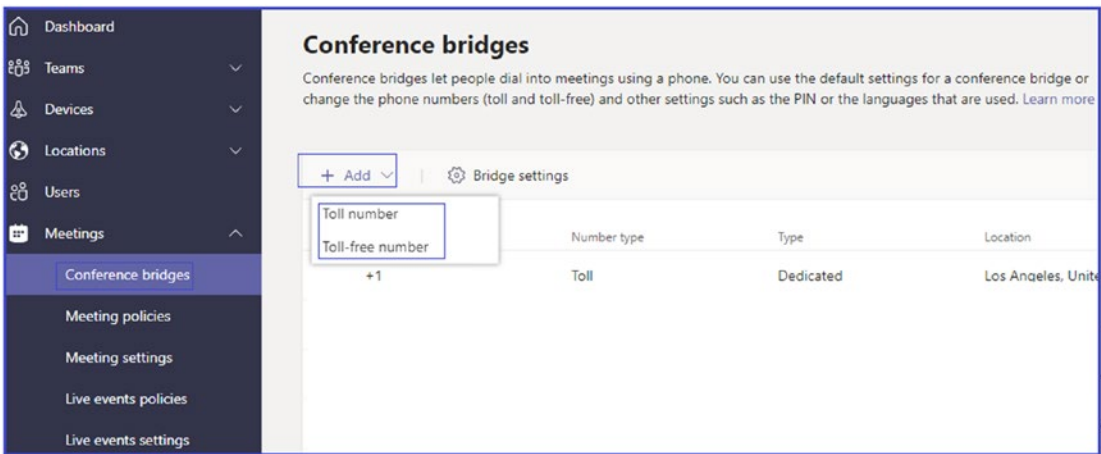


Figure 4-12. Adding a conference bridge number

Setting a Default Conference Bridge Number

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

1. On the Conference Bridges page, in the main pane that shows all the conference bridge phone numbers, select the phone number you want to configure as your default.
2. Click Set As Default on the menu bar, as shown in Figure 4-13.

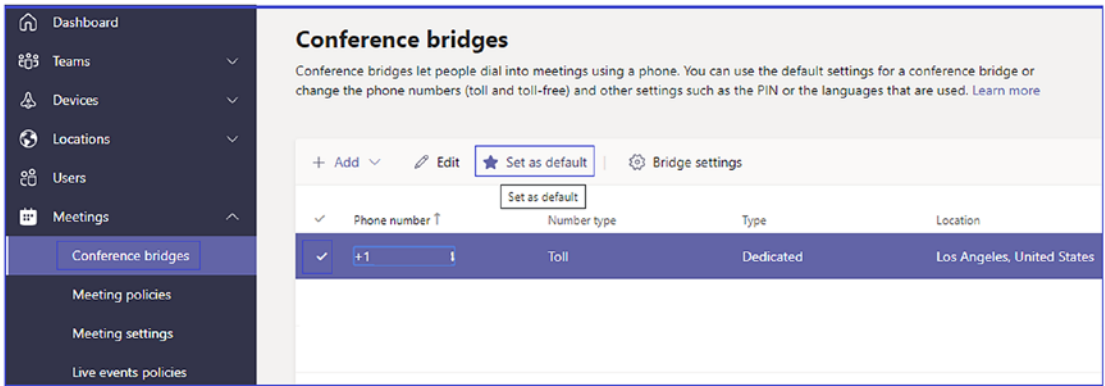


Figure 4-13. Setting a default conference bridge

Configuring and Managing Teams Conference Bridge Settings

To configure conference bridge settings, follow these steps.

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

- c. *PIN Length*: Set the PIN length value between 4 and 12; the default value is 5.
 - d. *Automatically Send Emails To Users If Their Dial-in Settings Change*: This option should be enabled or disabled.
3. Finally, click Apply to confirm the settings, as shown in Figure 4-14.

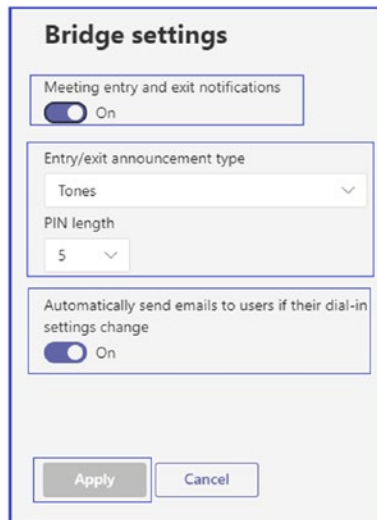


Figure 4-14. Conference bridge settings

Setting Up and Managing Communications Credits for Audio Conferencing

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

A Microsoft 365 Audio Conferencing license subscription offers 60 minutes per user per month that can be used to dial out to nonpremium numbers in any of the Zone A

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

Note All dial-out calls exceeding 3,000 minutes per calendar month are billed per minute using Communications Credits at Microsoft published rates to that destination [87].

Now you know when Communications Credits is going to be used in Teams Audio Conferencing. As an admin, you need to set up Communications Credits if you would like to use toll-free numbers with Microsoft Teams. Microsoft recommends that you set up Communications Credits for your Calling Plans (Domestic or International) and Audio Conferencing users who need the ability to dial out to any destination. Many countries and regions are included, but some destinations might not be included in the Calling Plan or Audio Conferencing subscriptions. If you don't set up Communications Credits billing and assign a Communications Credits license to your users and you run out of minutes for your organization (depending on your Calling Plan or Audio Conferencing plan in your country or region), those users won't be able to make calls or dial out from Audio Conferencing meetings [88].

Communications Credits provide a convenient way to pay for Audio Conferencing and Calling Plan minutes. It ensures users are never without the ability to add toll-free numbers to use with Audio Conferencing meetings, auto attendants, or call queues. Toll-free calls are billed per minute and require a positive Communications Credits balance. Dialing out from an Audio Conferencing meeting to add someone else from anywhere in the world requires dial-out credit. Additionally, Communications Credits gets used when users dial any international phone number when they have a Domestic Calling Plan subscription or dial international phone numbers beyond what is included in a Domestic and International Calling Plan subscription. Another important use case for Communications Credits is dialing out and paying per minute once you have exhausted your monthly minute allotment.

Assigning Communications Credits to a User

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

Checking Communications Credits Plans and Pricing

Before setting Communications Credits, you must check the plans and pricing. To do so, log in to the Microsoft 365 admin center (<https://portal.office.com/adminportal/home?add=sub&adminportal=1#/catalog>) and navigate to Billing ► Subscriptions ► Add Subscriptions and validate the subscription plans.

Setting Up Communications Credits for a Tenant

Next you need to know how to set up Communications Credits for your organization. To do so, follow this procedure.

1. Log in to Microsoft Office 365 admin center (<https://admin.microsoft.com/Adminportal/Home?>) with your work or school account. Click Billing and then select Purchase Services. Scroll down and select Add-Ons.
2. Select Communications Credits. On the Communications Credits subscription page, enter your information, and then click Next.

3. In the Add Funds Field, enter the amount that you want to add to your account.
4. Microsoft recommends enabling the Auto-Recharge option. It automatically refills your account when the balance falls below the threshold that you set. If you don't enable this setting, once the funds are used, calling capabilities that are enabled using Communications Credits will be disrupted (e.g., inbound toll-free service). Auto-recharge avoids the need to manually add a Communications Credits balance each time your balance reaches zero. In the example in Figure 4-15, this feature is selected, and \$100 in funds has been added for Bloguc Organization.

Checkout

How does this look?

Communications Credits

A convenient way to pay for Calling Plan minutes not covered and toll free numbers. [Get more info](#)

Add funds
What you should know before adding funds

USD(\$) 100

Auto-recharge
Turn on auto-recharge so you don't lose PSTN service unexpectedly. Auto-recharge adds funds automatically when your balance falls below a certain amount.

Recharge amount		Recharge with	\$ 20
Trigger amount	When the balance falls below		\$ 50
Total			\$100

Additional taxes may apply. See your invoice for details.

Figure 4-15. *Communications Credits*

5. In the Recharge Amount field, enter the amount in the Recharge With box that you want added to your account once it reaches the trigger amount. The example in Figure 4-15 shows a value of \$20.

6. In the Trigger Amount field, enter the amount in the When The Balance Falls Below box that will be used to initiate the auto-recharge. Once your balance falls below this amount, the recharge amount will be added automatically to your account. In the example in Figure 4-15, the amount shown is \$50.

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

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

Checking a Tenant’s PSTN Usage

Every organization will have a different usage rate because usage is dependent on call volume and rates the provider charges. As an admin, you will need to get this type of usage data from your current PSTN service provider. For organizations using Skype for Business Online and Microsoft as a PSTN service provider, you can get usage data by reviewing it in either Microsoft 365 admin center ► Reports or Skype for Business admin center ► Reports ► PSTN Usage Details.

When you are setting up Communications Credits, you will need to examine call usage details for your organization to determine the amounts you will need. You can get call usage information by reviewing the PSTN usage details report. This report lets you export the call data records to Microsoft Excel and create custom reports.

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

To manage an individual user's conference bridge number, first log in to Teams admin center and navigate to Users. Find the individual user whose conference bridge number you want to check, and then under Account view the Audio Conferencing settings for the individual, as shown in Figure 4-16.

The screenshot displays the user profile for Balu Ilag in the Teams Admin Center. The profile includes a profile picture, contact information (phone number: +1408, email: bilag@bloguc.com), and a 7-day activity summary showing 10 meetings and 6 calls. The Audio Conferencing settings are highlighted in a blue box and include the following details:

- Audio conferencing:** On (with a link to "Send conference info in email")
- Conference ID:** Dynamic (with a link to "Reset conference ID")
- PIN:** ***** (with a link to "Reset PIN")
- Default conferencing toll phone number:** +1 - - - - -
- Invites from this user can include toll-free number:** On
- Default conferencing toll-free phone number:** Not assigned
- Dial-out permission:** Any destination

Figure 4-16. Audio Conferencing settings

Under Audio Conferencing, click Edit to modify the settings. On the Audio Conference page, turn on Audio Conferencing, modify the Toll Number or Toll-Free Number values, and modify the Dial-Out From Meetings setting if required. Figure 4-17 shows the settings for this example.

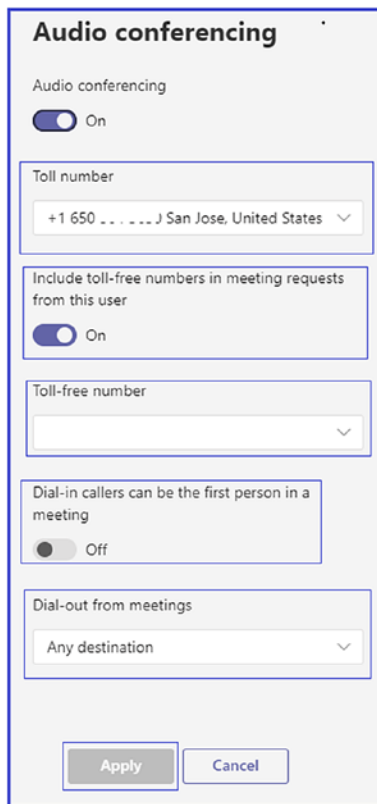


Figure 4-17. Modifying a conference bridge number for an individual user

Configuring and Managing Meeting Policies

Teams meeting policies provide the way to permit or restrict features that will be available to users during the 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. Next you need to determine which groups of users receive which meeting policies. Finally, you must determine whether your organization must purchase and deploy room system devices for your conference rooms.

As a Teams admin you need to manage meeting policies to control the features of meetings that the users within your organization are scheduling. 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 user's 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 meeting organizer:* All meeting participants receive the policy of the organizer.
- *Per user:* Only the per-user policy applies to restrict certain features for the organizer or meeting participants.
- *Per organizer and per user:* Certain features are restricted for meeting participants based on their policy and the organizer's policy.

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

Teams Phone System Planning

Microsoft Teams provides multiple capabilities, such as chat, audio and video calling, meetings, content sharing, phone calls to external numbers, and so on. One of the features is to make outbound phone calls through voice cloud that are delivered from Office 365 and provide Private Branch Exchange (PBX) functionality with opportunities for connecting to PSTN. The Microsoft Teams technology that allows call control and PBX capabilities is called Phone System.

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

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

- *Teams Direct Routing:* Using Direct Routing you can connect your existing on-premises PBX infrastructure with the Office 365 Phone System.
- *Teams Calling Plan:* Using Calling Plan, users can make and receive phone calls directly through Office 365 Phone System as a telephony provider by purchasing a Microsoft Calling Plan (domestic or domestic and international) for Office 365.

Configuring and Managing Teams Direct Routing

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

If your organization has an on-premises PSTN connectivity solution, for example, Bloguc Organization using Ribbon SBC to connect an ATT SIP trunk, Direct Routing enables you to connect a supported SBC to 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 PBX, analog devices, and Microsoft Phone System [57].

Figure 4-18 shows on-premises PSTN connectivity with a Microsoft Teams client using the Direct Routing capability.

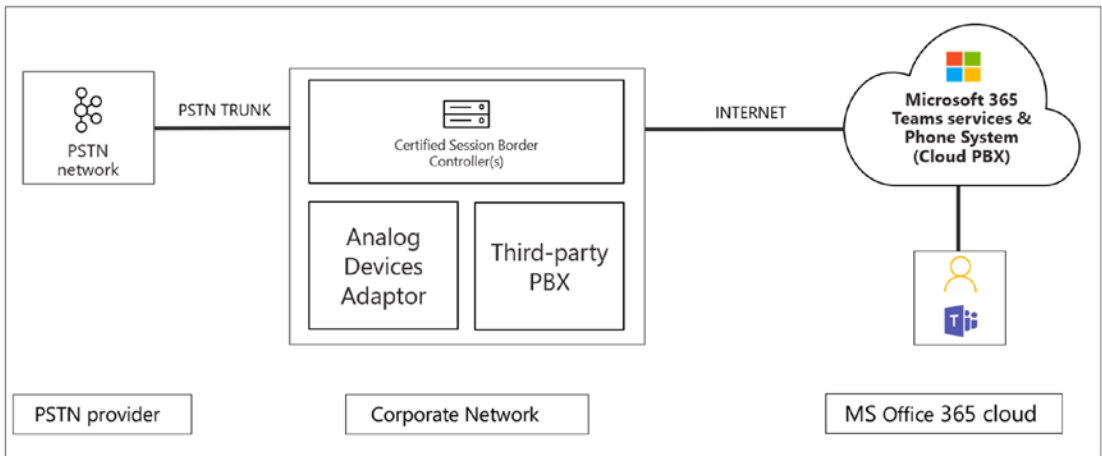


Figure 4-18. Teams Direct Routing connectivity

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

Configuring and Customizing Online PSTN Gateway for Microsoft Teams Direct Routing

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

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

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

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

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

-Identity

Every SBC has a unique name that is used for identifying the SBC. When creating a new SBC, the identity is provided through the `-FQDN` parameter. If the parameter is not defined, the identity will be copied from the `-FQDN` parameter, which means that an identity parameter is not mandatory [90].

For example, this command doesn't define identity, but it is copied from the `Fqdn` switch. That means identity is optional. `switch New-CsOnlinePSTNGateway -Fqdn sbc1.bloguc.com -SipSignallingPort 5061 -MaxConcurrentSessions 100 -Enabled $true`

-InboundPSTNNumberTranslationRules

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

-InboundTeamsNumberTranslationRules

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

-OutboundPSTNNumberTranslationRulesList

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

-OutboundTeamsNumberTranslationRulesList

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

-SipSignalingPort

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

-Fqdn

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

-ForwardCallHistory

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

-ForwardPAI

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

For example, the command looks like this: `New-CsOnlinePSTNGateway -Fqdn sbc1.bloguc.com -SipSignallingPort 5061 -MaxConcurrentSessions 100 -ForwardPAI $true -Enabled $true`

-Enabled

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

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

For example, `New-CsOnlinePSTNGateway -Fqdn sbc1.bloguc.com
-SipSignallingPort 5061 -MaxConcurrentSessions 100 -Enabled $true`

-ExcludedCodecs

This parameter allows some codecs to be excluded when media is being negotiated between Media Proxy and SBC.

-FailoverResponseCodes

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

-FailoverTimeSeconds

This parameter has a default value of 10. Outbound calls that are not answered by the PSTN gateway within 10 seconds are routed to the next available trunk; if there are no additional trunks, then the call is automatically dropped. In an organization with slow networks and slow gateway responses, that could potentially result in calls being dropped unnecessarily. As an admin, you can decide what failure time should be set for the SBC.

-Force

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

-ForwardPai

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

-GatewaySiteLbrEnabled

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

-GenerateRingingWhileLocatingUser

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

-MaxConcurrentSessions

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

-MediaBypass

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

-SendSipOptions

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

There are additional PowerShell commands to manage online PSTN gateway settings such as `Set-CsOnlinePSTNGateway`, `Get-CsOnlinePSTNGateway`, and `Remove-CsOnlinePSTNGateway` [90].

Figure 4-19 shows the online PSTN gateway PowerShell command parameters.

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

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

Figure 4-19. Teams PSTN gateway

Configuring and Managing Teams Calling Plans

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

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

- *Domestic Calling Plan:* Using this plan, Teams licensed users can call out to external phone numbers located in the country or region where they are assigned in Office 365.
- *Domestic and International Calling Plan:* Using this plan, Teams licensed users can call out to external phone numbers located in the country or region where their Office 365 license is assigned based on the user's location, and to international numbers in supported countries or regions. Currently, Calling Plan is available in 196 countries or regions that you can dial into using an international number.

Figure 4-20 shows the Microsoft-provided PSTN and Calling Plan plus Teams Phone System and the Office 365 cloud where corporate as well as remote users are connected for Teams services and phone calling capabilities.

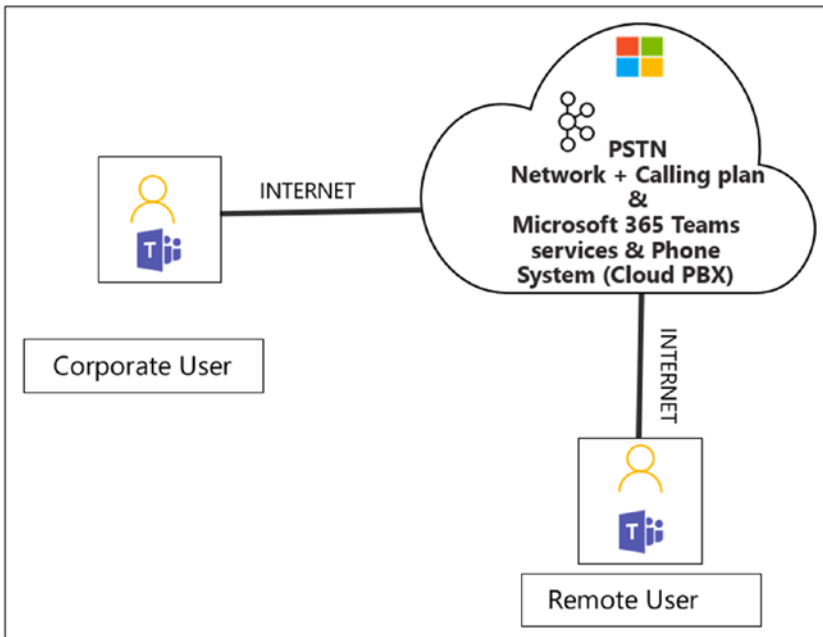


Figure 4-20. Teams Calling Plan

Setting Up a Calling Plan

Teams Calling Plan enables Teams users to make and receive phone call. However, as a Teams admin you must know how to set up Calling Plan. To set up this feature in your Teams environment, perform the following steps [89].

1. Check to determine whether Calling Plans are available in your country or region before they are purchased. Calling Plans can be purchased depending on availability per country or region. Therefore, when planning for your telephony solution, you should verify whether the country or region used in your Office 365 billing location supports Teams Audio Conferencing.
 - a. To check if Calling Plans are available in your country or region, visit this site, which shows the countries where Calling Plans are available: <https://docs.microsoft.com/en-us/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans/country-and-region-availability-for-audio-conferencing-and-calling-plans>.

2. Purchase and assign licenses. Once you ensure that Calling Plans are available and can be purchased for your country or region, you should buy the Calling Plan licenses and assign them to your users.
 - a. To purchase the Calling Plans license, visit <https://docs.microsoft.com/en-us/microsoftteams/calling-plans-for-office-365> to get more information.

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

3. Without a phone number, you cannot call in or call out; hence you have to acquire phone numbers. Teams provides several ways to get phone numbers.
 - *Use the Teams admin center:* This process is used when your country or region supports getting phone numbers through the Teams admin center.
 - *Port existing phone numbers:* This process is used if you want to port your existing phone numbers from the current carrier to the Office 365 Phone System.
 - *Use the request number for port numbers:* This process is used when the Teams admin center in your country or region does not support getting phone numbers.
4. Add emergency addresses and locations for the organization.
5. Assign a phone number and emergency address for the user.

Purchasing a Calling Plan for a Teams Organization

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

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

Important You can buy and assign different Calling Plans to different users, depending on the needs of your organization. After you select the Calling Plan you need, proceed to checkout and purchase the same and then you can assign a Calling Plan to each user in the Microsoft 365 admin center.

Assigning Calling Plan to Users

After acquiring Calling Plan licenses, you as an admin must assign the Calling Plan license to users using the calling service. To do so, log in to Microsoft 365 admin center and navigate to Users. Select Active Users and then find the user to whom you need to assign a Calling Plan license. Open that user account, select the appropriate license, and then click Save Changes. The example in Figure 4-21 shows an account with the Domestic and International Calling Plan assigned.

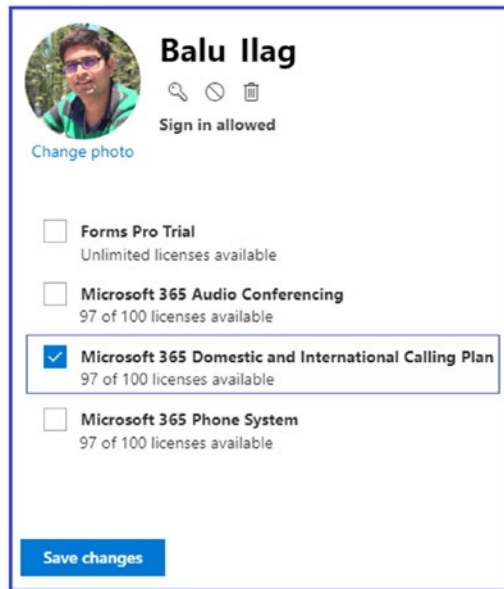


Figure 4-21. Assigning a Calling Plan

Configuring and Managing Call Queue

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

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

- With attendant routing, the first call in the queue rings all agents at the same time.
- With serial routing, the first call in the queue rings all call agents one by one.

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

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

Creating a Call Queue

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

- You must have a resource account created for the call queue.
- When you assign a phone number to a resource account, you can use the cost-free Phone System Virtual User license, officially called the Microsoft 365 Phone System Virtual User.
- Another important requirement is to assign a phone number. Remember that you can only assign toll and toll-free service phone numbers that you got in the Microsoft Teams admin center or transferred from another service provider to cloud call queues.
- Additionally, Communications Credits setup in Microsoft 365 is required for toll and toll-free service numbers [91].

Follow these steps to create a call queue.

1. Get service numbers from Microsoft or transfer your existing toll or toll-free service phone numbers before you create your call queues. Once you get the toll or toll-free service phone numbers, they will show up in Microsoft Teams admin center under Voice ► Phone Numbers.
2. Create a resource account. Every call queue must have an associated resource account, and then you can associate it with the call queue. You should perform the following steps to create a new call queue:
 - a. Go to the Microsoft Teams admin center, select Voice. Select Call Queues, and then click + Add New.
 - b. On the Call Queues \ Add, page give the call queue a meaningful display name that will be displayed notifications for incoming calls. Figure 4-22 shows TestCall Queue1 as the queue name.

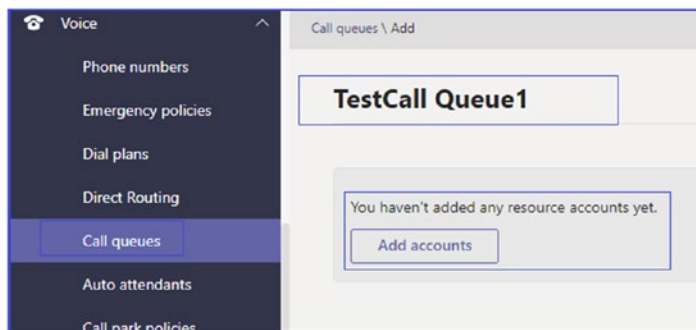


Figure 4-22. Call queue name and selecting a resource account

- c. Click Add Accounts to select a resource account (it may or may not be associated with a toll or toll-free phone number for the call queue, but each call queue requires an associated resource account). If no resource accounts are listed, you will have to get service numbers and assign them to a resource account before you can create this call queue. In this example, we assume that resource account is associated.
3. Set the greeting and music that will be played while a call is on hold, as shown in Figure 4-23.

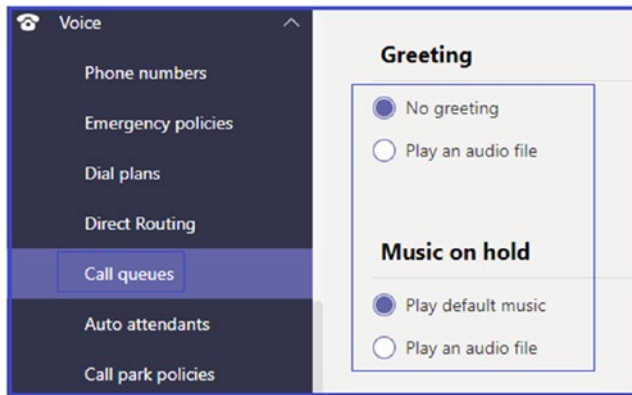


Figure 4-23. Select a greeting and music on hold

4. Select the call answering options. You can select a user agent or group. Up to 200 call agents can belong to an Office 365 Group, security group, or distribution list. The example in Figure 4-24 shows Balu Ilag as the call agent.

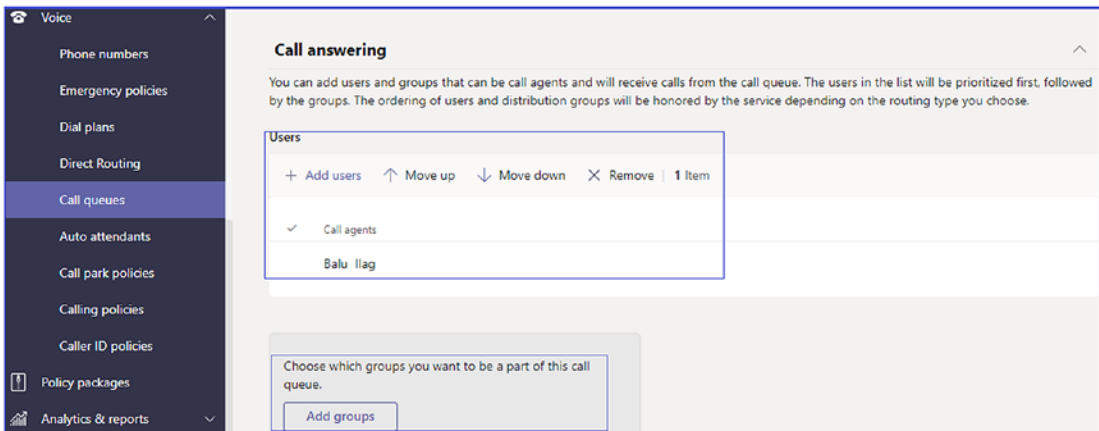


Figure 4-24. Selecting an agent

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

5. Next, select a routing method for your call queue distribution method. You can select from the following options.
 - a. *Attendant Routing*: This enables the first call in the queue to ring all call agents at the same time. The first call agent to pick up the call gets the call.
 - b. *Serial Routing*: Using this option, an incoming call rings call agents one by one, starting from the beginning of the call agent list (agents cannot be ordered within the call agent list). If an agent dismisses or does not pick up a call, then the call will ring the next agent on the list, trying all agents one by one until it is picked up or times out waiting in the queue.
 - c. *Round Robin*: Using this method balances routing of incoming calls so that each call agent gets the same number of calls from the queue. Figure 4-25 shows the round robin method selected. Agents Can Opt Out Of Taking Calls is set to On, and the Agent Alert Time setting is 35 seconds.

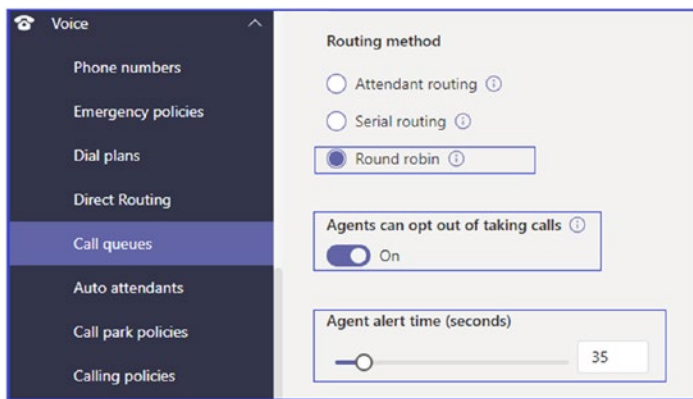


Figure 4-25. Routing method selection

6. For call overflow handling, you can configure the Maximum Calls In The Queue setting to set the maximum number of calls that can be in the queue at the same time (the default is 50, but

the value can range from 0 to 200). When the call queue reaches the maximum you have set, you can select what happens to new incoming calls using the following options.

- a. *Disconnect*: This option will disconnect the call.
- b. *Redirect To*: Using this option, select one of the following redirect settings.
 - 1. *Person In Organization*: This selection, shown in Figure 4-26, enables you to select the person to whom the incoming call will be redirected, and the call will be forwarded directly to voicemail.
 - 2. *Voice Application*: You must select the name of an existing resource account associated with either a call queue or an auto attendant.

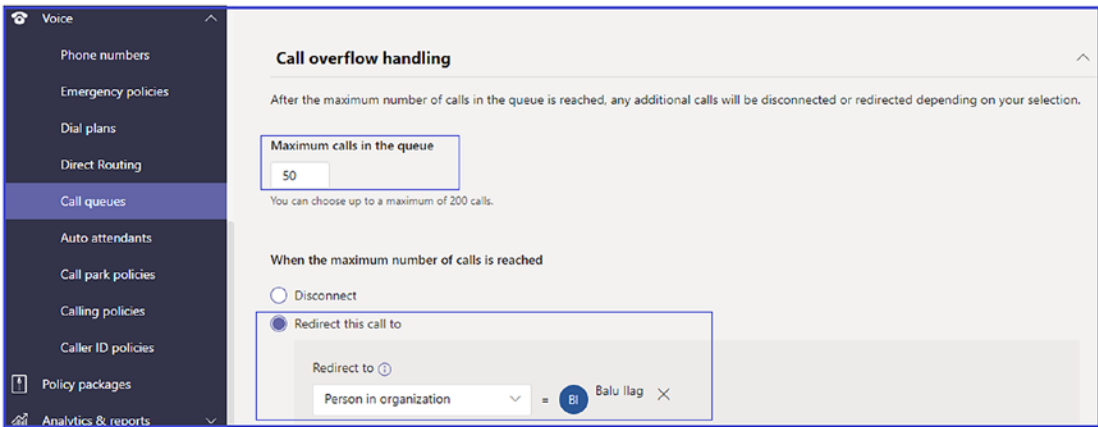


Figure 4-26. Call overflow handling

Note As of this writing, you cannot redirect calls to an external PSTN number.

- 7. The last setting to configure is call time out handling. This enables you to set up how long a call can be placed on hold in the queue before it times out and needs to be redirected or disconnected (where it is redirected will depend on your When Call Times Out setting). You can set a value from 0 to 45 minutes, and the timeout

value can be set in seconds, at 15-second intervals. When a call reaches the limit, you can choose what happens to it based on the following options.

- a. *Disconnect*: This option, selected in Figure 4-27, will disconnect the call.
- b. *Redirect This Call To*: Select one of the following redirect options:
 - i. *Person In Your Company*: This option enables you to select the person to whom the incoming call will be redirected, and the call will be forwarded directly to voicemail.
 - ii. *Voice Application*: You must select the name of an existing resource account associated with either a call queue or an auto attendant.

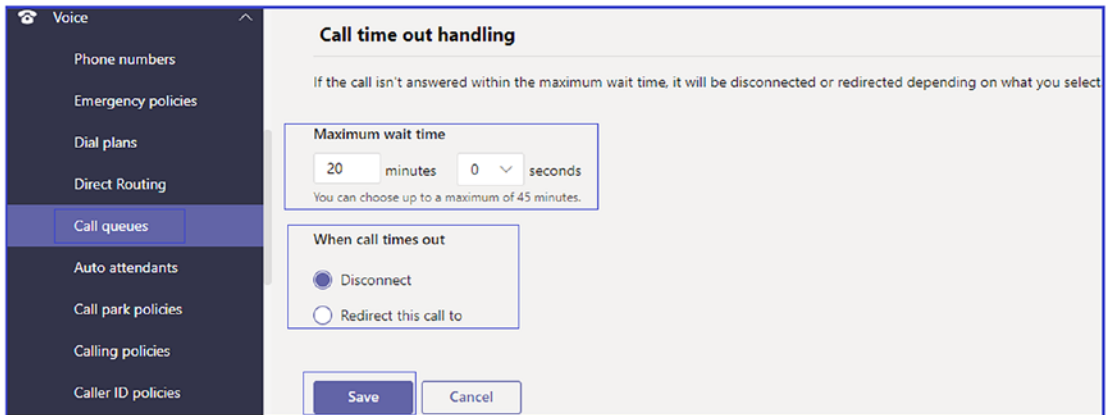


Figure 4-27. Call time out handling

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

Managing a Call Queue

To manage a call queue, a Teams admin needs to visit the Teams admin center. Log in to Teams admin center, select Voice, and then select Call Queue. On the Call Queue

page you will see all the call queues listed. You need select the call queue that you want to manage. On the Call Queue page you can add a new call queue, edit an existing call queue, or delete a call queue (see Figure 4-28).

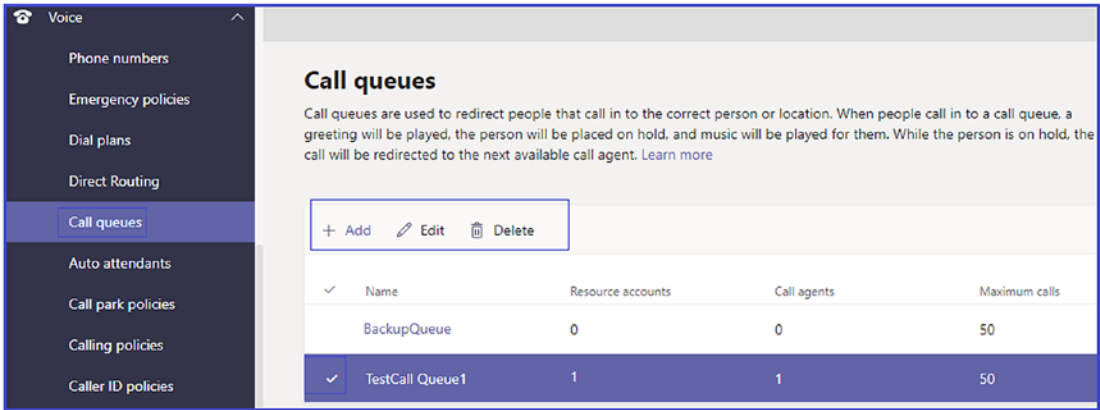


Figure 4-28. Call queue management options

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

Managing and Configuring Auto Attendant in Teams

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

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

Auto attendant does have some prerequisites before creation.

- An auto attendant must have an associated resource account.
- When assigning a phone number to an auto attendant, you are assigning it to the resource account that has been associated with that auto attendant; this enables you to have more than one phone number that can access an auto attendant.
- Most often, a resource account will use the cost-free Phone System Virtual User license.
- To get and use toll-free service numbers for your auto attendants, you must set up Communications Credits.
- A complete auto attendant system usually involves multiple auto attendants and might only require a single assigned phone number for the top-level or entry auto attendant.
- You can apply more than one phone number to an auto attendant by associating more than one resource account to the auto attendant.

Creating Auto Attendant with an Existing Resource Account

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

1. Log in to the Teams admin center and navigate to Voice. Select Auto Attendant and click Add.
2. On the Auto Attendants \ Add Auto Attendant page, shown in Figure 4-29, enter a meaningful name and provide the following information.
 - *Operator*: This setting specifies whether a user can request to talk to a person or voice app, or if there will be no designated operator. You can refer people to another auto attendant, a call queue, or an enterprise voice-enabled Skype for Business or Teams user.

- *Time Zone:* This specifies time zone in which the auto attendant will calculate business hours and holidays.
- *Language:* This setting specifies the language the system will use.
- *Enable Voice Input:* This enables voice navigation in the auto attendant menu.

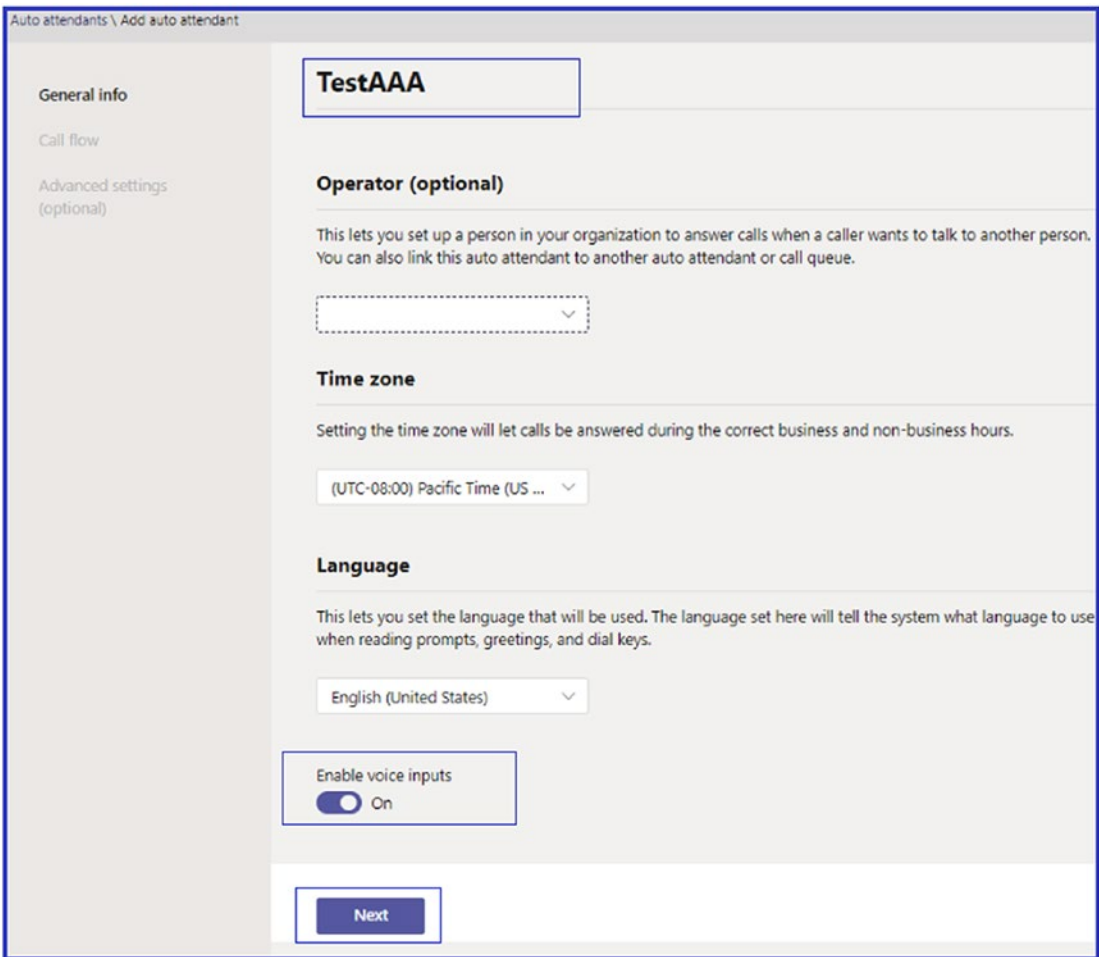


Figure 4-29. Adding an auto attendant

3. Click Next. On page that opens, you are asked to configure the following settings.
 - *First Play A Greeting Message:* You can select No Greeting, Play An Audio File, or Type In A Greeting Message. Figure 4-30 shows an example of a greeting message entered.

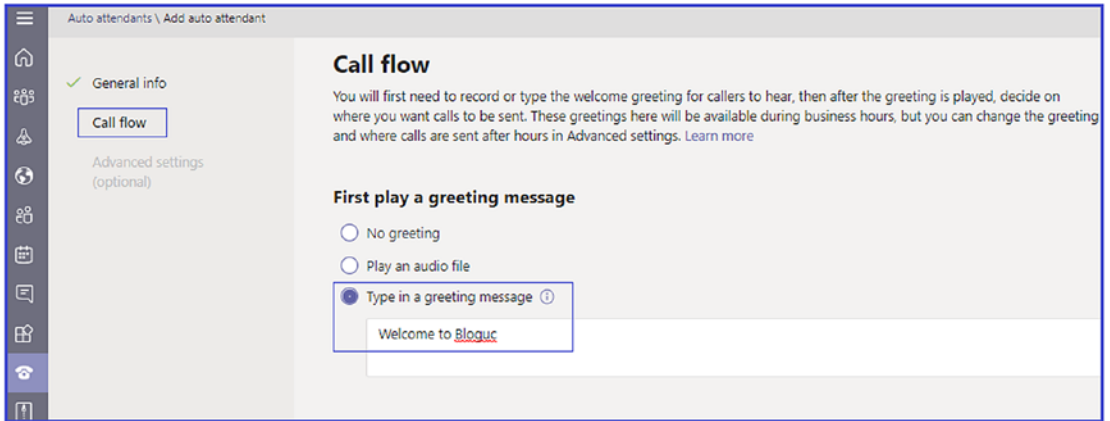


Figure 4-30. *Typing in a greeting message*

- *The Route The Call:* You can redirect the call, disconnect the call, or play the menu options, as shown in Figure 4-31. If you play the menu options, you will be able to configure which options are open to the caller and how he or she can choose among them. The caller can use dial keys or voice input to navigate the options, and you can redirect the caller to auto attendants, call queues, or users. You can also allow users to search your directory.

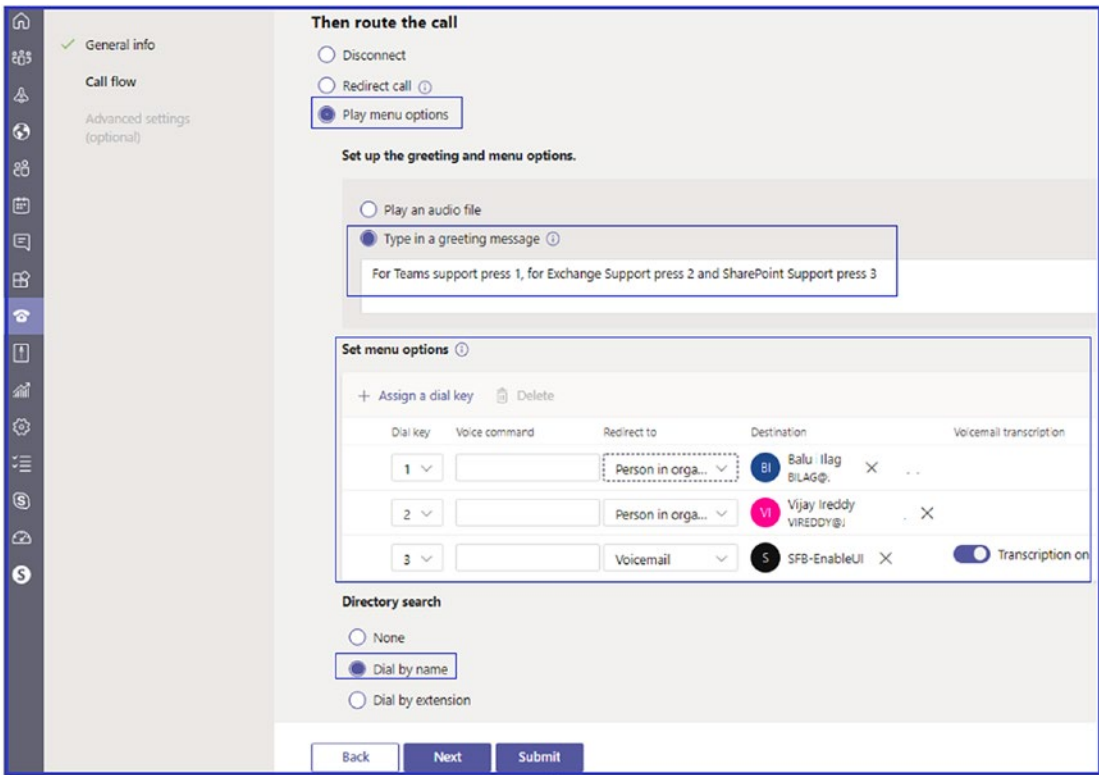


Figure 4-31. Call routing options

4. Click Next. On the next page, shown in Figure 4-32, provide the following information.
 - *Set Business Hours:* Use these settings to specify when the auto attendant will be considered working. If you do not provide any business hours, the auto attendant will be set to 24/7 by default.
 - *Set Up After Hours Call Flow:* Select what will happen to the call outside of business hours. If you do not change the default setting, your call will disconnect outside of business hours.
 - *First Play A Greeting Message:* Specify a greeting for calls that are received outside of business hours. If you do not change the default setting, your call will not play an outside of business hours greeting.

Set business hours

By default, business hours are set to 24/7, Monday through Sunday. If you set custom business hours, all hours that aren't included in business hours are considered after business hours.

Reset to default Clear all hours

Day	Start at	End at	
Sunday	12:00 AM	12:00 AM	+ Add new time
Monday	12:00 AM	12:00 AM	+ Add new time
Tuesday	12:00 AM	12:00 AM	+ Add new time
Wednesday	12:00 AM	12:00 AM	+ Add new time
Thursday	12:00 AM	12:00 AM	+ Add new time
Friday	12:00 AM	12:00 AM	+ Add new time
Saturday	12:00 AM	12:00 AM	+ Add new time

Set up after hours call flow

If you have business hours set up, you will need to also set up what to do with the call when it's answered during after hours.

First play a greeting message

No greeting

Play an audio file

Type in a greeting message ⓘ

Back Next Submit

Figure 4-32. set business hours

5. Click Next. On the next page you can click + Add to add specific dates as holidays for your auto attendant. Then you will be asked to provide the following information, as shown in Figure 4-33.
 - *Name:* Select the name for the holiday option.
 - *Date:* This is the date for the holiday.
 - *Greeting:* You can elect not to play a greeting, and instead play an audio file or use text to speech.
 - *Actions:* You can decide to disconnect or redirect calls.

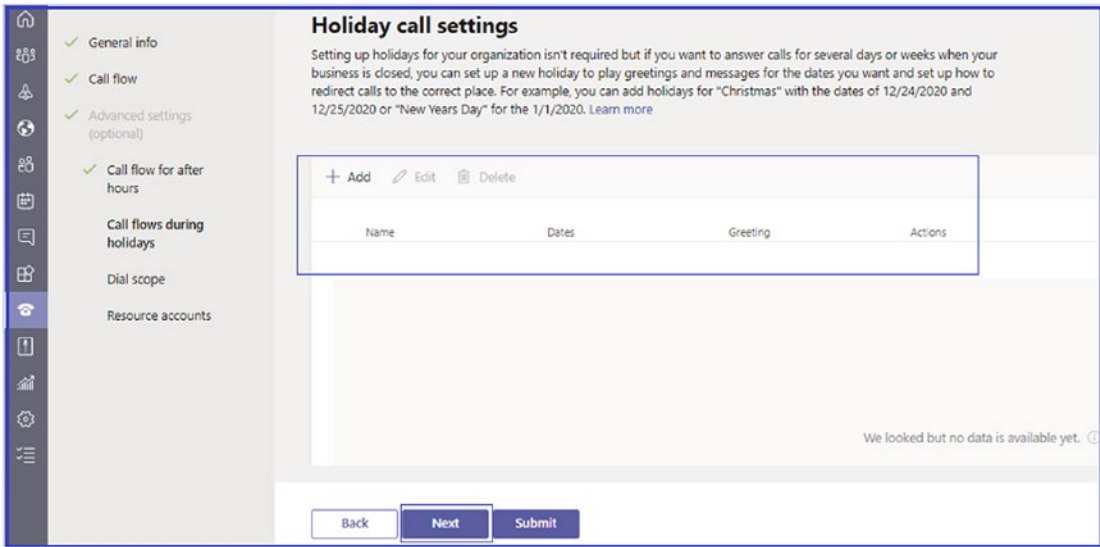


Figure 4-33. *Holiday call settings*

6. Click Save to save the holiday. You can add multiple holidays by repeating Steps 5 and 6.
7. Click Next. On the page that opens you can define the scope of users that is searchable by the caller, as displayed in Figure 4-34.
 - *Include:* Select a group of users or all online users. Online users are all the users whose accounts are online or those who have been added using Azure directory sync. Custom groups can be security, distribution, and Office 365 Groups.
 - *Exclude:* You can select None or Custom User Group. This will exclude those users from being searchable.

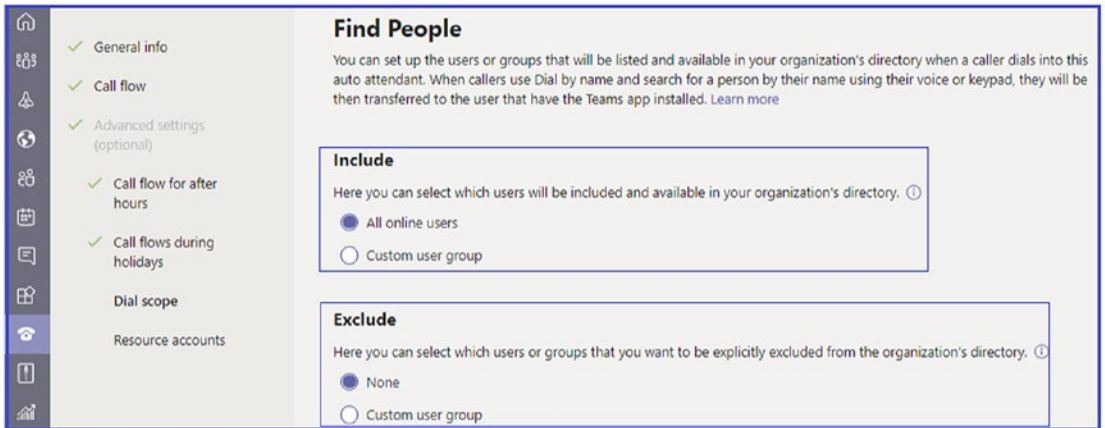


Figure 4-34. Find people settings

8. Click Next. On the next page you will be asked to assign at least one resource account to the auto attendant. Click Add Accounts (see Figure 4-35) and search for the account you already created in the right panel. If you have yet to create an account, you can select Add Resource Account after searching for a nonexistent account name.

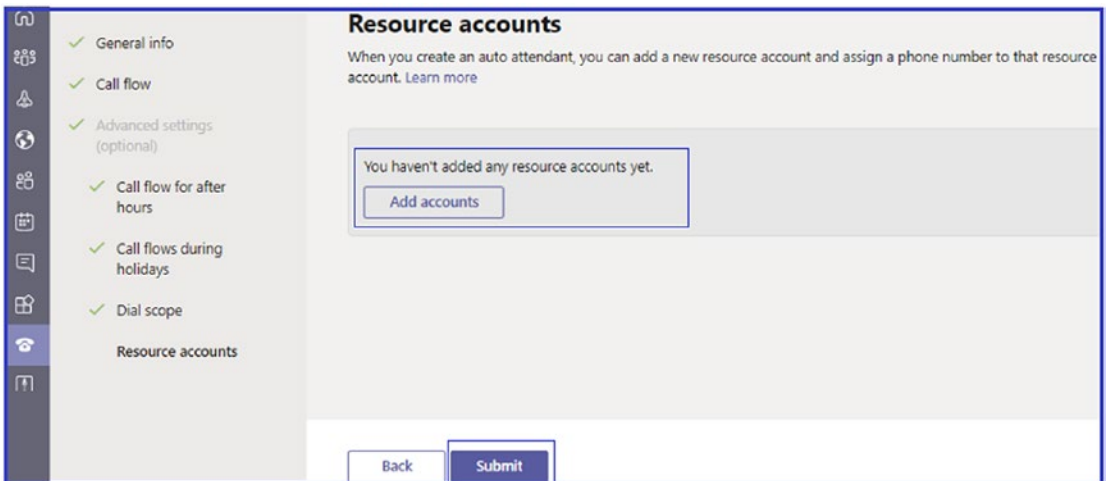


Figure 4-35. Adding a resource account

9. Click Add to add the existing resource account to the attendant. Click Submit to create your auto attendant.

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

Managing Auto Attendant

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

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

Assigning Phone Numbers for an Auto Attendant

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

To assign a service number, you must first get or port your existing toll or toll-free service numbers. Once you get the toll or toll-free service phone numbers, they show up in Microsoft Teams admin center ► Voice ► Phone Numbers. You can identify these numbers by looking for the type listed as Service.

Searching for Users

When searching for users as part of the auto attendant functionality, callers can search by name or by extension. This functionality is also known as directory search.

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

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

Maximum Directory Size

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

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

With dial by extension, the caller needs the full extension number.

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

Setting Menu Options

You can assign functions for the 0–9 dial keys in an auto attendant using the Skype for Business admin center. Different sets of menu options can be created for business hours and after hours, and you can enable or disable dial by name in the menu options. Keys can be mapped to transfer the calls to any of the following:

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

Configuring and Managing Emergency Calling

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

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

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

First you need to understand the different terminology used here. First, the emergency address is a civic address containing the physical or street address of a place of business for your organization. For example, the Bloguc Organization HQ office address is 537 South Tradition Street, Tracy, CA 95391. Although not an emergency address, a place can also be used. The place is typically used when an office facility contains multiple floors, buildings, office numbers, and so on. A place is associated with an emergency address to give a more exact location within a building [92].

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

Configuring Emergency Location in the Teams Admin Center

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

1. Log in to Teams admin center. Navigate to Location and then select Emergency Addresses. Click + Add.
2. Enter the name and a meaningful description for an address, as illustrated in Figure 4-36. Once you are finished, click Save to commit the changes.

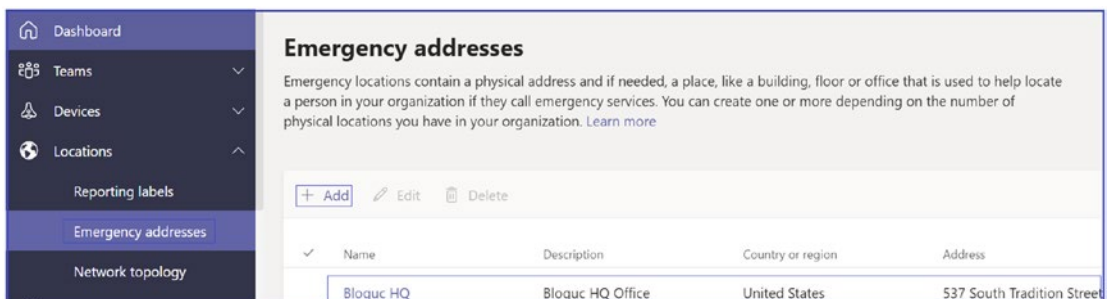


Figure 4-36. Adding an emergency address

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

Validating Emergency Addresses

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

When you enter an emergency address by using the address map search feature in the Microsoft Teams admin center, the address is automatically marked as validated. Remember, you cannot modify a validated emergency address. If the address format changes, you must create a new address with the updated format. After emergency address validation, the address will be marked as validated and then you can assign this address to an end user account or network identifier. Figure 4-37 shows that the Bloguc HQ office address has been validated.

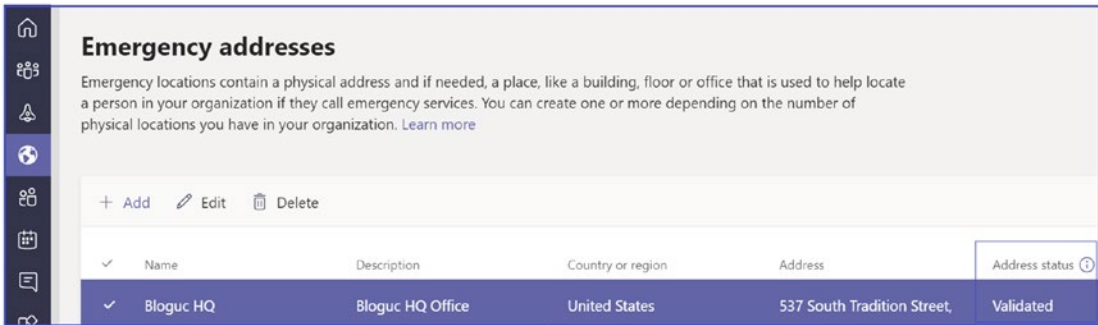


Figure 4-37. Emergency address status

Configuring Emergency Calling in Calling Plan Environment

There are multiple considerations you need to understand before you configure emergency calling, including emergency addresses, dynamic emergency addresses, and emergency call routing.

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

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

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

Another consideration is using dynamic emergency calling. This feature allows end users to have their location information sent along with the call to emergency services. To use dynamic emergency calling, a Teams admin must define the organization's network topology to identify the location of the client endpoint. For example, Balu usually works from the Tracy office location, so when he makes a call to emergency services, his Tracy office address is sent to the PSAP. Sometimes, however, he works from a Sacramento office location. If he makes a call to emergency services when he is in the Sacramento office, then the dynamic emergency calling service will send his Sacramento office address to the PSAP based on his network identifier that exists on the network [92].

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

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

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

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

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

Considerations for Emergency Phone System Direct Routing

Microsoft Teams supports emergency calling service through Teams direct routing. Basically, Teams allows you to use your existing phone system, including SBC with PSTN connectivity, for inbound and outbound phone calling. As a Teams admin, you must understand how emergency calling works using Direct Routing, and then you can decide to use Direct Routing for emergency calling. You must define emergency calling policies for Direct Routing users using the `TeamsEmergencyCallRoutingPolicy` PowerShell command to define emergency numbers and their associated routing destination.

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

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

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

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

- For emergency call routing in a Teams Direct Routing scenario, the `TeamsEmergencyCallRoutingPolicy` mentions an online PSTN usage, which should have the appropriate Direct Routing configuration to properly route the emergency calls to the appropriate PSTN gateway(s) using online PSTN routes. As a Teams admin, you should make sure that there is an `OnlineVoiceRoute` for the emergency dial string.
- The ability to dynamically route emergency calls for Direct Routing users varies depending on the emergency calling network in each country. Two solutions are available: Emergency Routing Service Providers (ERSPs; U.S. only) and Emergency Location Identification Number (ELIN) gateway applications.

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

Configuring Dynamic Emergency Call Routing Using Direct Routing

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

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

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

Step 1: Preparation Work

1. As a Teams admin, you must configure the network settings and the LIS to create a network and emergency location map. Specific to Direct Routing, additional configuration is required for routing

emergency calls and possibly for partner connectivity. you must configure connection to an ERSP (in the United States) or configure the SBC for an ELIN application.

2. At startup, and periodically afterward or when a network connection is changed, the Teams client sends a location request that contains its network connectivity information to the network settings and the LIS.
3. If there is a network settings site match, emergency calling policies are returned to the Teams client from that site; if there is a LIS match—an emergency location from the network element—the Teams client it is connected to is returned to the Teams client.
4. Once the user using Teams client attempts an emergency call, the emergency location is conveyed to the PSTN and then for Direct Routing, you must configure the SBC to send emergency calls to the ERSP or configure the SBC ELIN application.
5. Another important consideration is the supported Teams client version, so users must be using one of the following Teams clients to use the emergency service.
 - Teams desktop client (Windows and macOS).
 - Teams mobile client for Apple iOS client version 1.0.92.2019121004 and App Store version 1.0.92 and greater.
 - Teams mobile client for Android client and Google Play Store version 1416/1.0.0.2019121201 and greater.
 - Teams phone version 1449/1.0.94.2019110802 and greater.

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

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

- The network region includes a set of network sites.

- The network site is a location where your organization has a physical office, such as an office, a set of buildings, or a campus. These sites are defined as a set of IP subnets.
- A network subnet should be associated with a specific network site. A Teams client's location is determined based on the network subnet and the associated network site.
- Trusted IPs are a collection of the external IPs (public-facing IPs also known NAT IPs) of the organization network and are used to determine if the user's endpoint is inside the corporate network.

WHEN DO I NEED TO CONFIGURE REGION, SITE, SUBNET, AND TRUSTED IP ADDRESSES?

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

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

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

Configuring Location information Service

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

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

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

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

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

Note Support for ether switches and ports is still not available. You can check Microsoft's official documentation for the same (<https://docs.microsoft.com/en-us/microsoftteams/configure-dynamic-emergency-calling>).

Configuring Emergency Policies

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

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

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

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

Follow this procedure to create a custom emergency calling policy.

1. Log in to Teams admin center and navigate to Voice. Select Emergency Policies, and then click the Calling Policies tab. Click Add. Enter a name and description for the policy. The example in Figure 4-38 shows Bloguc-EMS-Policy as the policy name.
2. On the same page you can set how you want to notify people in your organization, typically the security desk, when an emergency call is made. To do this, 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:* Using this option, users can participate.

If you selected the Conferenced In But Are Muted notification mode, in the Dial-Out Number For Notifications box, you can enter the PSTN phone number of a user or group to call and join the emergency call. For example, enter the number of your organization's security desk (this example uses +1209000111 as the Bloguc security desk number), who will receive a call when an emergency call is made and can then listen in or participate in the call.

3. Search for and select one or more users or groups, such as your organization's security desk, to notify when an emergency call is made. The example in Figure 4-38 lists alert@bloguc.com. The notification can be sent to email addresses of users, distribution groups, and security groups. A maximum of 50 users can be notified.
4. Click Save to commit the changes.

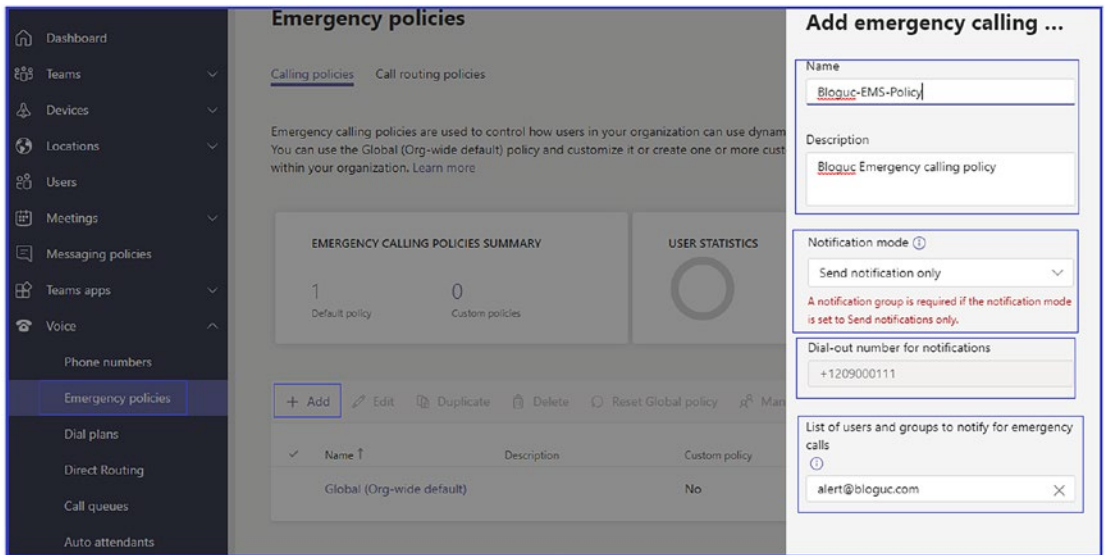


Figure 4-38. *Emergency policies*

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

If you assigned an emergency calling policy to a network site and to a user and if that user is at that network site, the policy that is assigned to the network site overrides the policy that is assigned to the user [93].

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

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

```
$en = New-CsTeamsEmergencyNumber -EmergencyDialString "911"
-EmergencyDialMask "911;9911" -OnlinePSTNUsage "Local" -CarrierProfile
"Local"
New-CsTeamsEmergencyCallRoutingPolicy -Identity "HQ-Emergency" -Tenant
$tenant -EmergencyNumbers @{add=$en} -AllowEnhancedEmergencyServices:$true
-Description "HQ Emergency Route Policy"
```

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

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

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

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

Managing Phone Numbers

Acquiring and Managing Teams Service Numbers and User Phone Numbers

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

- *Teams service numbers:* These numbers are assigned to services such as Audio Conferencing, auto attendants, and call queues. Service phone numbers, which have a higher concurrent call capacity than

user numbers, will vary by country or region and the type of number (whether it is a toll or toll-free number). Admins can acquire service (toll or toll-free) numbers from Microsoft.

- *Teams user phone numbers:* User phone numbers can be assigned to users in the organization for inbound and outbound calling purposes. As an admin, you can acquire Teams user phone numbers from Microsoft or port your existing phone number to Microsoft and use it in Teams Phone System along with Calling Plan.

Getting a Service or Phone Number

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

1. Log in to Teams admin center, then navigate to Voice and click Phone Numbers.
2. On the Phone Numbers page, under Numbers, click + Add for a new phone number request. Enter a name and description.
3. In the Location And Quantity section, enter the following information, as shown in Figure 4-39.
 - *Country Or Region:* Select country or region.
 - *Number Type:* Select the appropriate option that determines whether the phone numbers are designated for users or for services, such as conference bridge, call queue, or auto attendant.
 - *Location:* Choose a location for connecting the new phone numbers. If you need to create a new location, select Add A Location and enter the required location's data.
 - *Area Code:* Select a valid area code for the country and location.
 - *Quantity:* Enter the number of phone numbers that you want for your organization.

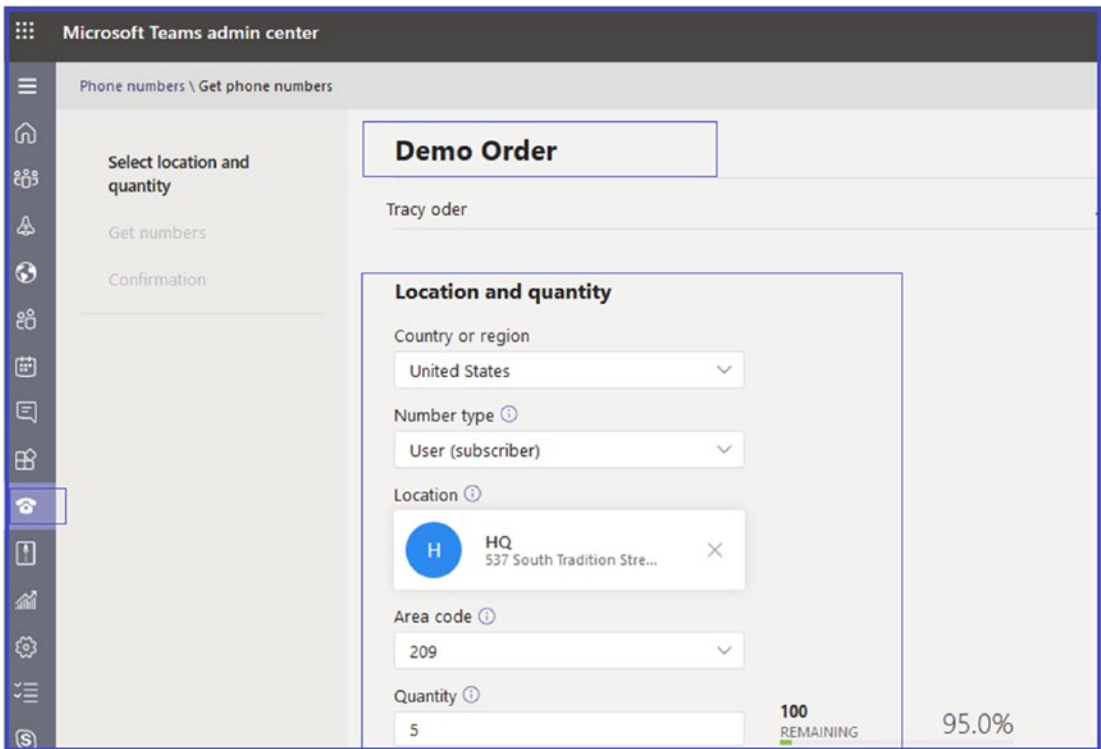


Figure 4-39. Phone number order

4. Click *Next* to continue. On the Get Numbers page, select the phone numbers you want to apply to your tenant.
5. Click Place Order to submit the order.

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

Creating and Managing Voice Routing Policy

As an Teams admin, you must know how to create and manage Teams voice routing policies. Teams Phone System has a routing mechanism that allows a call to be sent to a specific SBC based on the called number pattern plus the specific user who makes

the call. SBCs can be designated as active or backup controllers. When the SBC that is configured as active is not available for a specific call route, then the call will be routed to a backup SBC [94].

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

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

Follow these steps to create a voice routing policy.

1. First create PSTN usage (one or more) for voice routing policy. Remember that, as of this writing, you cannot create a voice routing policy or PSTN usage or routes using Teams admin center. You will have to use Windows PowerShell. Before running the following PowerShell command, however, you must connect PowerShell to Skype for Business Online and Teams tenant. To connect PowerShell to Skype for Business Online and Teams module, you must install it (see <https://docs.microsoft.com/en-us/skypeforbusiness/set-up-your-computer-for-windows-powershell/download-and-install-the-skype-for-business-online-connector>). After you install the connector, run the following sample command to connect PowerShell with Skype for Business Online and Teams (you must change the domain name).

```
Import-Module skypeonlineconnector
$sfboSession = New-CsOnlineSession -OverrideAdminDomain "bloguc.
onmicrosoft.com"
Import-PSSession $sfboSession -AllowClobber
```

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

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

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

```
New-CsOnlineVoiceRoute -Identity "Tracy1" -NumberPattern
"^\\+1(209|210)
(\\d{7})$" -OnlinePstnGatewayList sbc1.bloguc.com, sbc2.bloguc.com
-Priority 1 -OnlinePstnUsages "US East and US West"
```

```
New-CsOnlineVoiceRoute -Identity "Tracy2" -NumberPattern
"^\\+1(209|210)
(\\d{7})$" -OnlinePstnGatewayList sbc3.bloguc.com, sbc4.bloguc.com
-Priority 2 -OnlinePstnUsages " US East and US West"
```

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

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

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

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

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

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

Tip As an admin, you can create a voice routing policy with multiple PSTN usages.

You can use the preceding PowerShell commands and make a script to assign policies to multiple users.

Summary

You have learned about Teams conference management including Audio Conferencing (dial-in) and VoIP for both internal and external attendees, and Teams Phone System management, including Teams Direct Routing and Calling Plan with voice routing policies.

CHAPTER 5

Microsoft Teams Governance and Life Cycle Management

You have already learned that Microsoft Teams is built on Office 365 Groups, which is part of Office 365 that includes multiple tools to design governance capabilities that organizations require. This chapter provides you with a comprehensive overview of Microsoft Teams governance and life cycle management. Managing governance and life cycle management for Teams is essential for consistent and coordinated interaction between users and allows them to collaborate with confidence. Prior to deploying Teams, you as a Teams admin must consider things, like who can create teams, how to handle unused Teams, who can create private channels, what the Teams naming convention is, and so on. Also, you will learn the features that you can use for Teams governance, such as group creation, classification, expiration policy, sensitivity labels, data loss prevention policies, and naming policy.

After completing this chapter, you will be able to do the following.

- User provisioning Configure and manage conditional access policy.
- Manage information protection using data loss prevention (DLP).
- Create and manage eDiscovery for Teams.
- Manage data governance and retention in Teams.
- Manage internal risk through information barrier (IB) in Teams.
- Create and manage Office 365 Group classification for Teams and Outlook.
- Create and manage Office 365 Group expiration policy for Teams.
- Create and manage Office 365 Group naming policy for Teams.

User Provisioning for Microsoft Teams

Before using Microsoft Teams and its features, each user must provision for Teams; without provisioning, users cannot avail themselves of Teams features. Teams user provisioning involves enabling Teams licenses as well as add-on licenses, including Phone System and Office 365 Audio Conferencing, and granting the required policies.

Enabling a User Teams License

To enable a Teams license for a user, as well as add-on licenses, follow this procedure.

1. Log in to Office 365 admin center and navigate to Users. Select Active Users and find the user to whom you need to assign a license. You can then enable all necessary licenses. Figure 5-1 shows user Balu Ilag with all required licenses needed to use Teams as a unified communication and collaboration tool.

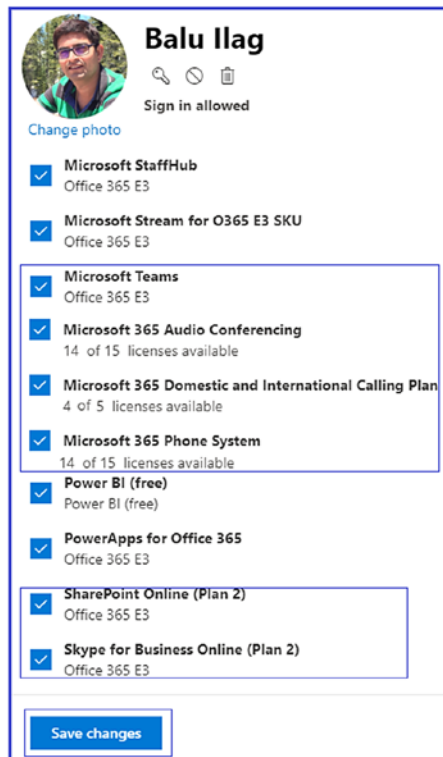


Figure 5-1. Enabling licenses for a user

As a Teams admin, you can manage user accounts in Office 365 admin center for modifying users' display attributes and passwords (depending on the organization topology). You can use the Teams admin center to assign and manage any Teams-specific policies such as meeting policy, live event policy, Teams policy, and so on. You can refer to Chapter 1 for an overview of licensing.

Assigning Meeting Policy to a User Account Using Teams Admin Center

You can assign or remove any policy from a user account using Teams admin center. This includes meeting policies, message policies, live event policies, emergency calling policies, and so on. Follow the steps to assign a Teams meeting policy. After you create a meeting policy, the next step is to assign the policy to a user. You can assign a meeting policy within the Teams Admin center in both the Users and Meeting Policy sections. Follow this procedure to assign a meeting policy in the Users section.

1. Log in to Teams admin center, and navigate to Users. Select the users to whom you want to apply the policy and then click Edit Settings.
2. In the Edit User Policies window, shown in Figure 5-2, select the required meeting policy, and then click Apply.

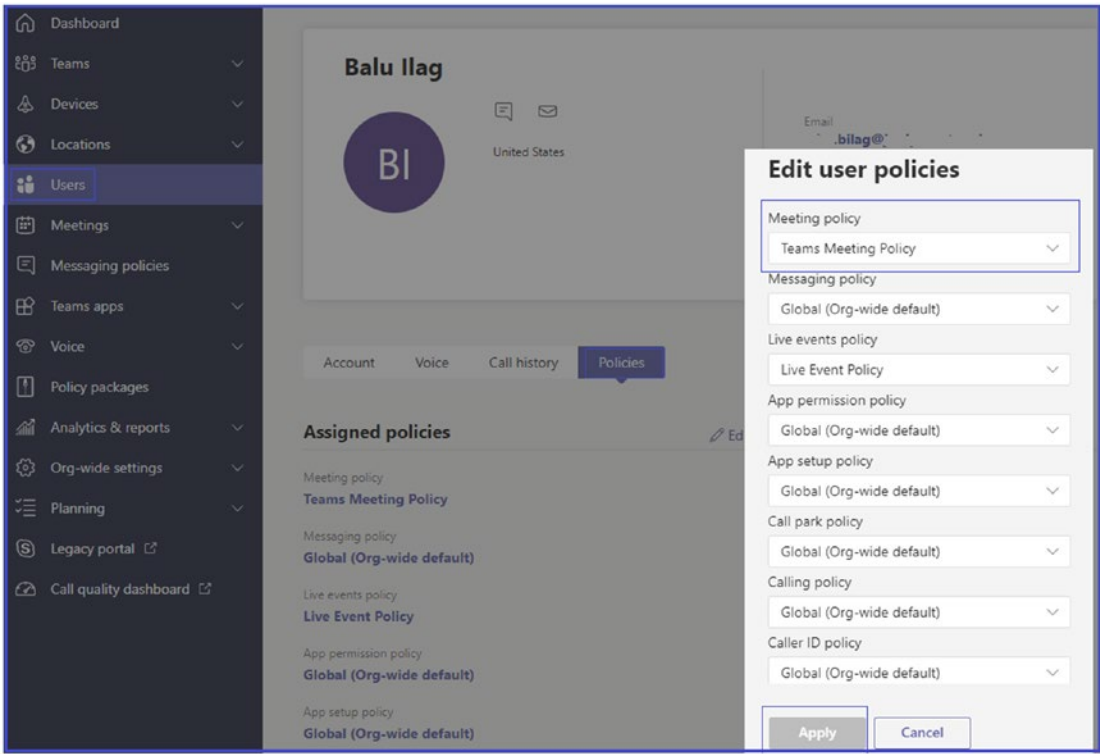


Figure 5-2. Assigning a meeting policy

You can also assign a meeting policy in the Meeting Policies section. To do so, log in to Teams admin center and then navigate to Meetings. Select the required meeting policy and then click Manage Users. In the Manage Users windows, select the user to whom to assign the policy, as shown in Figure 5-3. Click Apply.

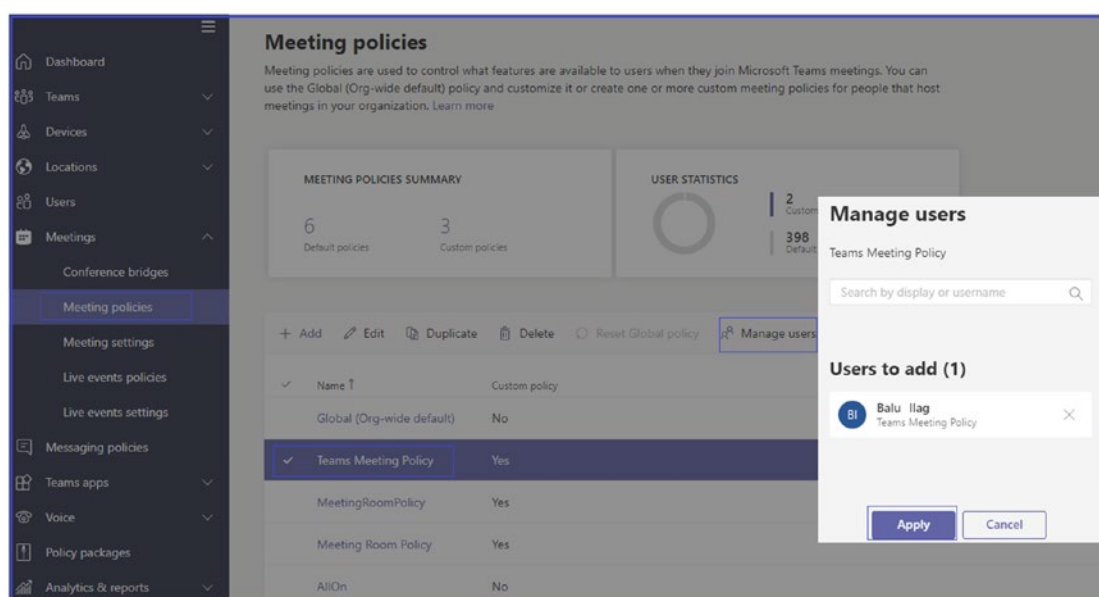


Figure 5-3. Assigning a policy using the Meeting Policies section

Third-Party Application and Policy Management

As a Teams admin, you must be aware of the apps that Teams has. Microsoft Teams apps offer multiple features that allow your organization to maximize its Teams experience. These apps include the functionality of tabs, messaging extensions, connectors, and bots provided by Microsoft, built by a third party, or created by developers in your organization. You can manage the apps using the Teams apps section in the Teams admin center, where you can set policies to manage apps for your organization. For example, you can set policies to control what apps are available to Teams users, and you can customize Teams by including the apps that are most important for your users. Figure 5-4 shows the available options to manage apps, manage permission policies, and set up new custom policies.

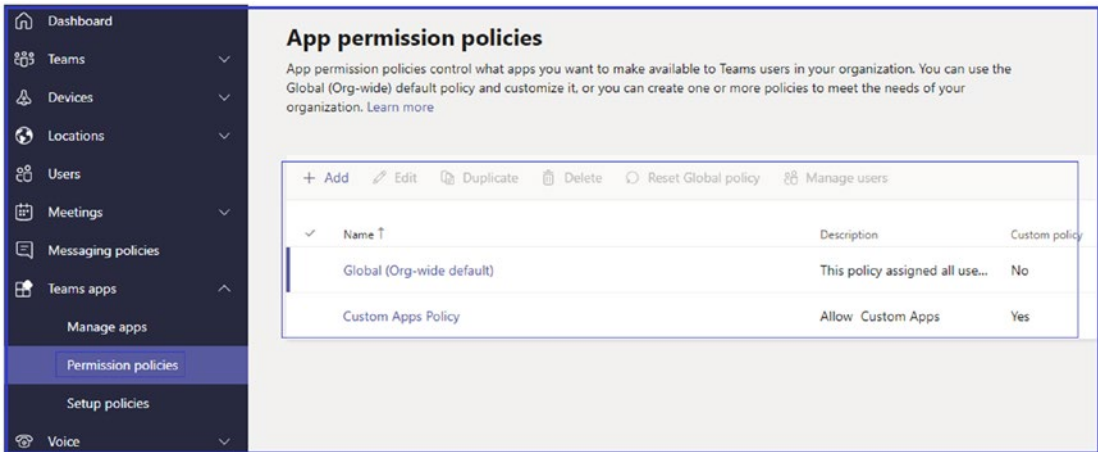


Figure 5-4. Teams apps and policies

Teams Apps Permission Policies

Using app permission policies, you can block or allow apps either organization-wide or for specific users. When you block an app, all collaborations with that app are disabled, and the app 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.

Managing the Custom App Setup Policies

Admins can use the Teams admin center to manage or edit a policy, including the Global (Org-wide default) policy and custom policies that admins have created. Follow this procedure to manage policies.

1. Log in to Teams admin center, and navigate to Teams Apps. Select Setup Policies and then select the policy you want to work with. Click Edit to manage the policy settings.
2. On the edit page, make the changes that you want. You can add, remove, and change the order of apps, and then click Save.

Assigning a Custom App Setup Policy to Users

You can use the Teams admin center to assign a custom app setup policy to individual users, or you can use the Skype for Business Online PowerShell module to assign a custom policy to groups of users, such as a distribution group or security group. There are multiple ways to assign an app setup policy to your users in the Teams admin center. You can assign users either in Setup Policies or in Users in Teams admin center.

To assign policies to users using the Teams admin center, follow these steps.

1. Log in to Teams admin center and navigate to Teams apps. Select Setup Policies.
2. Select the custom policy and then click Manage Users.
3. On the Manage Users page, search for the user by display name or by username, select the name, and then click Add. Repeat this step for each user who you want to add.
4. Once you are finished adding users, click *Apply*.

Creation and management of custom policies for apps was covered in Chapter 2.

Teams Governance and Life Cycle Management

So far you have learned how Microsoft Teams can change workplace collaboration, providing a centralized workplace for users to come together to chat, meet, call, create, and make decisions. Teams provides a single place where users can connect and organize teams or projects without disturbing other workflows. Teams also provides a single platform where users can access all business-critical information and applications, and automate their repeatable processes efficiently.

Organizations can bring their applications (custom apps), tools, and services into Teams, and Teams supports all of this work. As an admin, you can also connect everyone in your organization through the single platform of Teams, bringing together such diverse functions as technology organization, manufacturing flow, a classroom, and hospitals. Everyone can come together and leverage the power of Teams.

Teams and information security admins in your organization must be aware of what Teams provides to securely maintain the data that Microsoft Teams generates. When the data are generated, your concern as an administrator is who is accessing the data

and how it can be secured and accessed by only the users who need the data. Microsoft itself is investing a great deal in securing Teams data, and Teams benefits from the all security, compliance, and identity investments that Microsoft has already made in the information protection and compliance area.

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 able to respond to it, application of data governance policies, what type of content exists and how long it is retained, and finally the ability to manage the risks. This topic will provide you the information that you need to manage Teams governance and overall life cycle.

Microsoft Teams Identity and Access Management

Teams identity was already covered in Chapter 2, but a recap is in order. Identity management is crucial for any application or system. If bad actors compromise an identity, your data and content could be misused. Because Teams leverages Azure AD for identity, the investments and improvements in Azure are directly applied to Microsoft Teams.

Microsoft Teams has strong authentications because it uses smart protection policies and risk assessment to block threats. As a Teams admin or security 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 are automatically supported for Teams because Teams uses SharePoint and Exchange extensively. When a user tries to log in to Teams, he or she will be challenged for the two-factor workflow or whether you have a PIN enabled and both have the same workflow [95].

Another aspect of identity is what authorized users have access to. 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. Figure 5-5 shows conditional access based on the signal that comes from the devices, applications, and users. Microsoft determines the risk score, and as a Teams admin you configure the policies that determine who can access the Teams application based on the conditions applied.

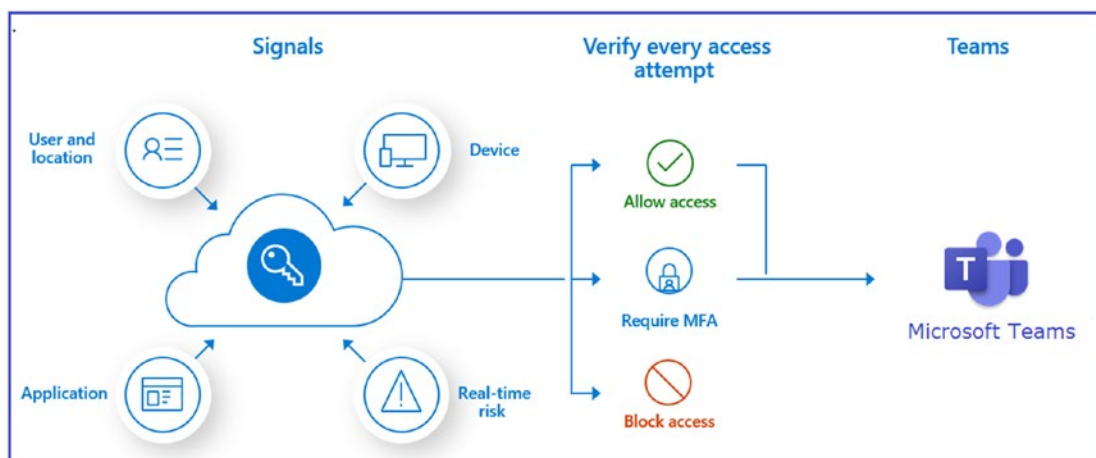


Figure 5-5. Conditional access workflow [22a]

Remember, the conditional access policies prevent access for authenticated users from unmanaged devices.

Configuring Conditional Access Policy for Microsoft Teams

Azure AD conditional access is a vast topic and includes many facets. For purposes of this book, I have designed an example conditional access policy. If you are interested in learning more about Azure AD and conditional access, refer to the Microsoft documentation at <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>.

Follow this procedure to implement a conditional access policy for Teams.

1. Log in to the Azure AD portal at <https://portal.azure.com>. You must have appropriate permission (e.g., Global admin role permission) to design conditional access.
2. On the Microsoft Azure home page, navigate to Conditional Access - Policies and open the link.
3. Click + New to create new conditional access policy. Enter a meaningful name so that the policy can be easily identified. For our test policy, the given name is CA for MS Teams.
4. Under Assignments, select the users and groups to which this policy will apply and then click Done. In the example in Figure 5-6, the user account selected is for Balu Ilag, bilag@bloguc.com.

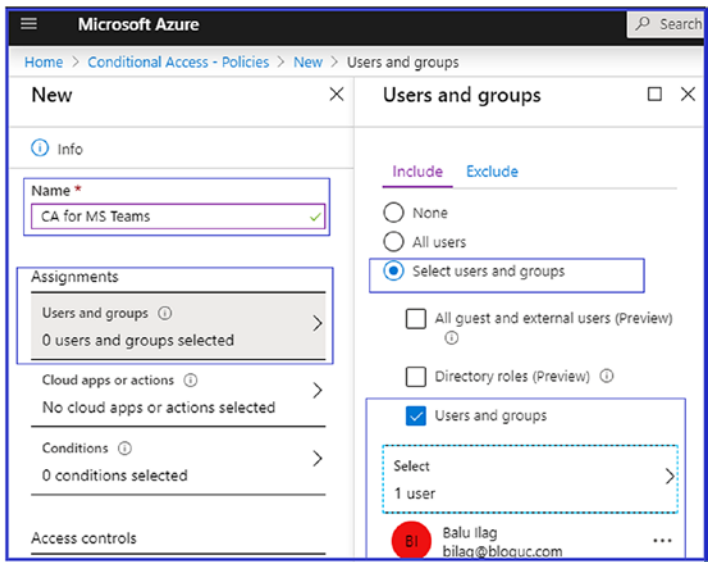


Figure 5-6. Conditional access policy assignment

5. In the Cloud Apps Or Actions pane, select Microsoft Teams as a first-party application. Select Microsoft Teams, as shown in Figure 5-7, and then click Done.

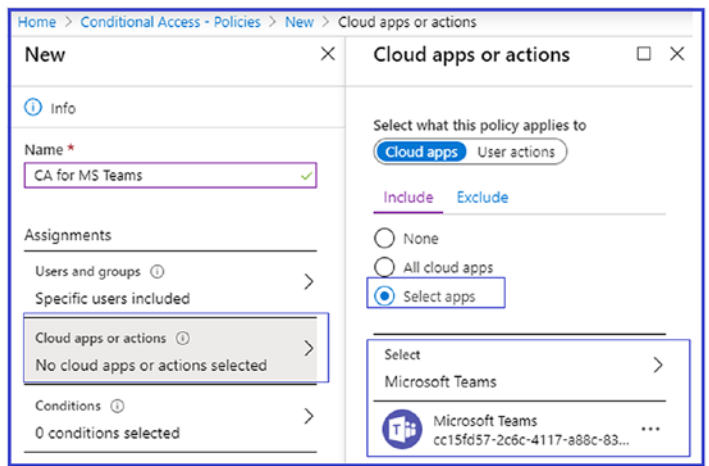


Figure 5-7. Cloud app as Teams

6. Select Conditions. In the Conditions pane, you will see different available options.
 - a. *Sign-in Risk*: This will allow you to select the sign-in risk level: High, Medium, Low, or No Risk. To enable this, set the toggle on Yes and then select the applicable sign-in risk. For the example shown in Figure 5-8, medium risk is selected. You can set risk as per your organization requirements.
 - b. *Device Platforms*: Select the platform, such as Any Device, or choose a specific platform—Android, iOS, Windows Phone, Windows, and macOS—to which to apply this policy. To enable this, first set the toggle to Yes and then select the platform. For the example test policy shown in Figure 5-8, Android, iOS, Windows Phone, Windows, and macOS device platforms are selected.
 - c. *Locations*: Select the location to control users' access based on their physical locations. To enable this, set the toggle to Yes and then select the location. For the example test policy in Figure 5-8, All Trusted Locations is selected. Click Done. You can select the location as per your organization requirement.
 - d. *Client Apps (Preview)*: Select the client app to which this policy is applied and then click Done. For this example, no client app is selected.
 - e. *Device State (Preview)*: Select the device state and then choose to enable this for all devices or exclude any devices and then click Done. For this example, test policy All Device State is selected.
 - f. Click Done to add the selected conditions, shown in Figure 5-8.

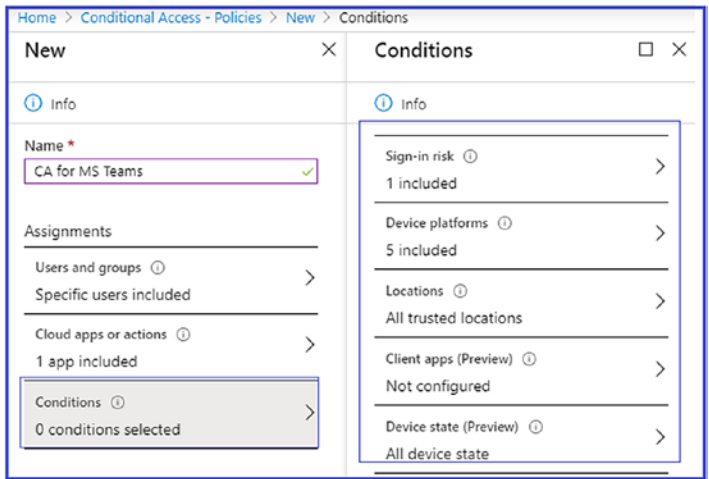


Figure 5-8. Conditions settings

7. *Access Controls:* Select the controls to be enforced, like Block or Grant. If Grant is chosen, then select Require Multi-Factor Authentication, Require Device To Be Marked As Compliant, Require Hybrid Azure AD Joined Device, and so on.
8. *Session:* The session controls enable limited experiences within a cloud app. Select the session usage requirements. For the example shown in Figure 5-9, Sign-In Frequency - 5 days is selected.
9. Click Create, as shown in Figure 5-9, to build this conditional access policy.

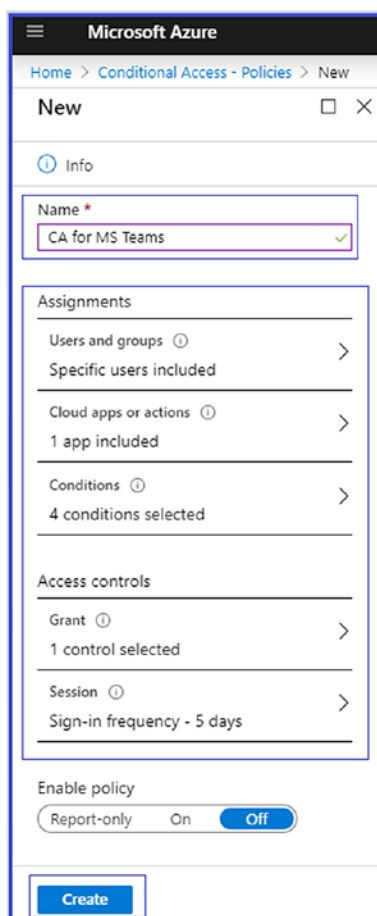


Figure 5-9. Creating a conditional access policy

User Experience When User Accesses the Teams Application

Figure 5-10 shows a warning message preventing users from accessing the Teams application from an unmanaged device. This is an example of the granular control that conditional access policy provides, preventing authorized users from accessing the Teams application from an unmanaged device. In this workflow, the first part is authorizing the user and the second part is applying conditions based on the policy to prevent a user from accessing the Teams app from an unmanaged device. Another valuable condition available through a conditional access policy is the prevention of Teams app access from nonwork locations.

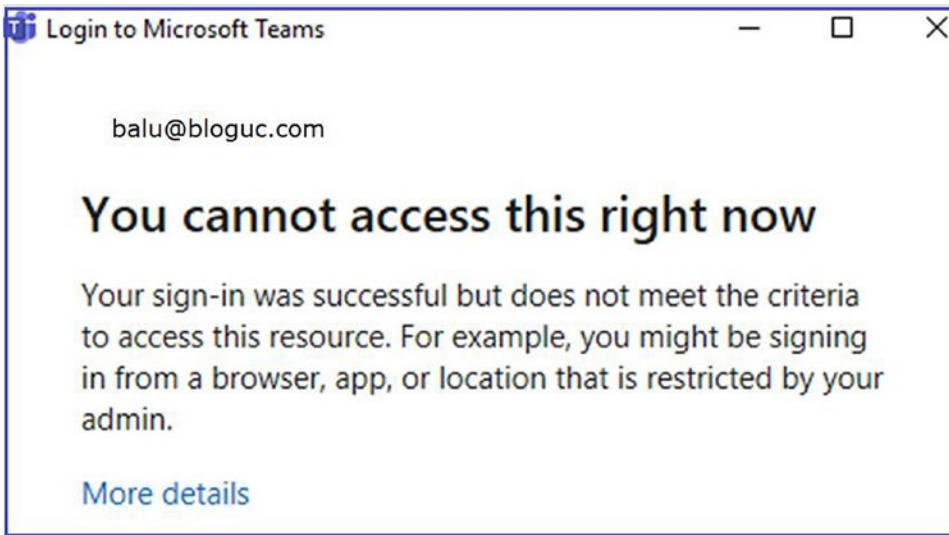


Figure 5-10. Teams app access blocked from an unmanaged device

Managing Information Protection Using Data Loss Prevention

In any application, an identity considered a front door. Once you secure the front door then you will be dealing with how to control the flow of information, and Teams is no exception. Microsoft Teams achieves information protection through the Office 365 data loss prevention (DLP) stack. DLP enables Teams and security admins to create policies to determine what is considered sensitive or nonsensitive information. Microsoft made this easier for admins by providing more than 80 predefined rules. An admin can leverage these existing predefined rules or create new custom rules or policy that an organization wants. You can monitor content, detect policy violations, and remediate violations as per the requirement.

Once you create policies, Teams monitors the content, and whenever a policy violation is detected, the end user gets notified, or you can set the policy to prevent access as well.

DLP Policies in Action

You can create DLP policies for different kind of workloads and enable them for Exchange, SharePoint, or Teams. There is only one portal to create DLP policies for all Office 365 applications, which means you don't have to switch among different portals for different applications.

As an example, two users from Bloguc Organizations are trying to share content. The sender is trying to send some content, but Bloguc Organization has already implemented a DLP policy that blocks the content because it includes sensitive information. The notification message to the sender, shown in Figure 5-11, says, “This message was blocked,” and also indicates why the content was blocked [99].

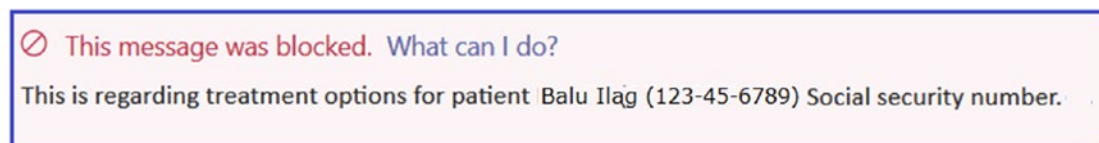


Figure 5-11. DLP policy blocked notification

The sender is also given the option to override the policy conditions and send the message or report it to a security admin. Figure 5-12 shows the override options.

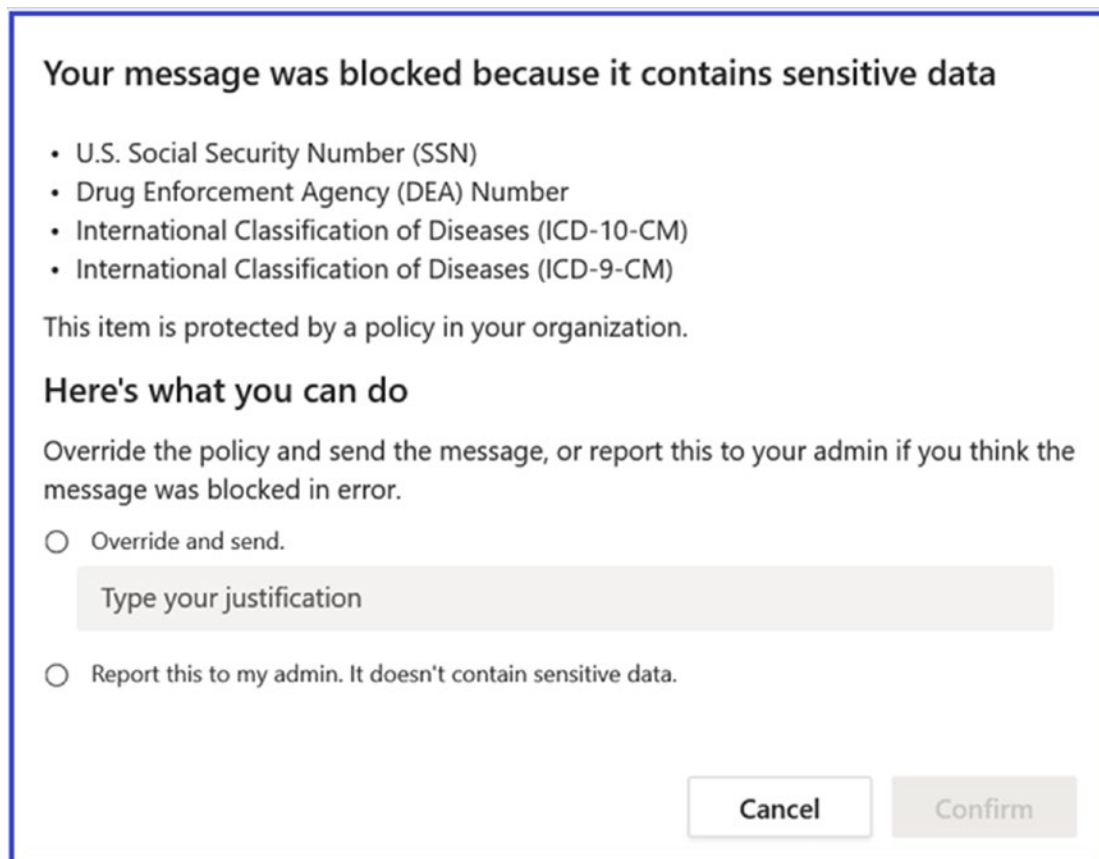


Figure 5-12. DLP policy override options [22a]

The receiver will just get the message saying “This message was blocked due to sensitive content,” as displayed in Figure 5-13.

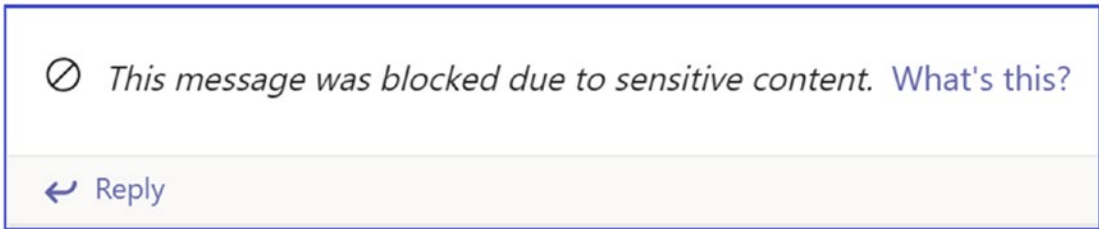


Figure 5-13. Message blocked due to sensitive content

This is considered a passive DLP solution, not active. You might wonder why it is considered passive. The reason is that when someone sends sensitive content, the receiver will see the content for a few seconds before it is removed from view. If you want to learn more, refer to the Microsoft documentation about DLP policies at <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies>, which helps explain why the message was blocked.

DLP policies are very useful and provide a solution for preventing the accidental sharing of critical information about confidential projects, both internally and externally.

As of this writing, to leverage DLP policies, both the sender and receiver should be moved to TeamsOnly mode. If the sender is in Island mode and the receiver is in TeamsOnly mode, then the DLP policy will not work the way it should. In addition, the time taken to block the content and generate the warning message is quite lengthy. Microsoft is working to reduce this delay.

Creating a DLP Policy for Microsoft Teams

Teams or security admins can create new or DLP policies or modify existing ones; however, you must have permission to execute the modification steps outlined here. Remember, by default, an organization’s tenant admin will have access to Security & Compliance Center, and they can give Teams or security admins and other people access to the Security & Compliance Center, without giving them all of the permissions of the tenant admin. To create a DLP policy follow this procedure.

1. Log in to Office 365 Security & Compliance Center by browsing to the site at <https://protection.office.com>. Select Data Loss Prevention and then select Policy. Click + Create A Policy. Figure 5-14 shows the Create A Policy option [23a].

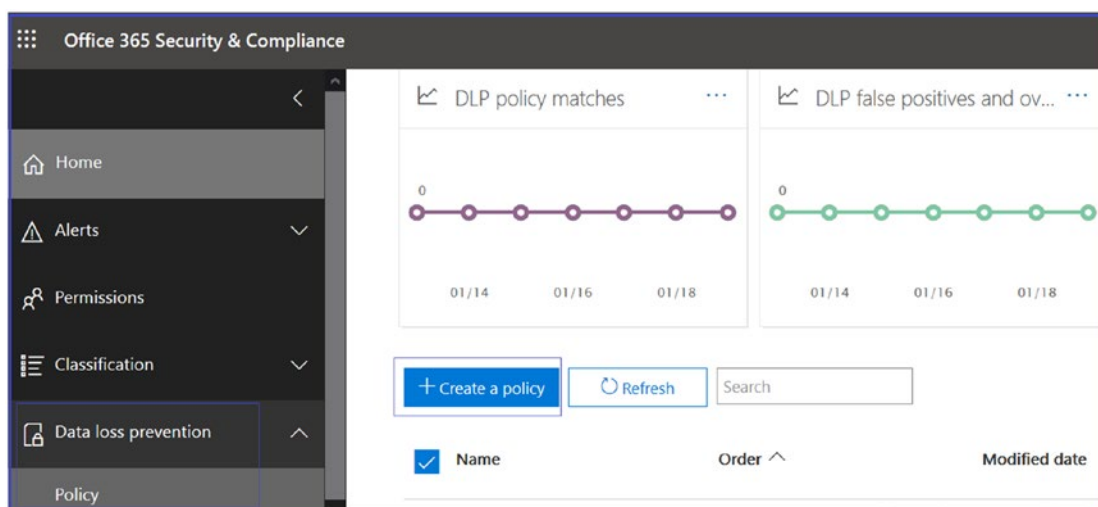


Figure 5-14. DLP policy creation options

2. Select a template, and then click Next. In the example shown in Figure 5-15, the U.S. Personally Identifiable Information (PII) Data template is selected.

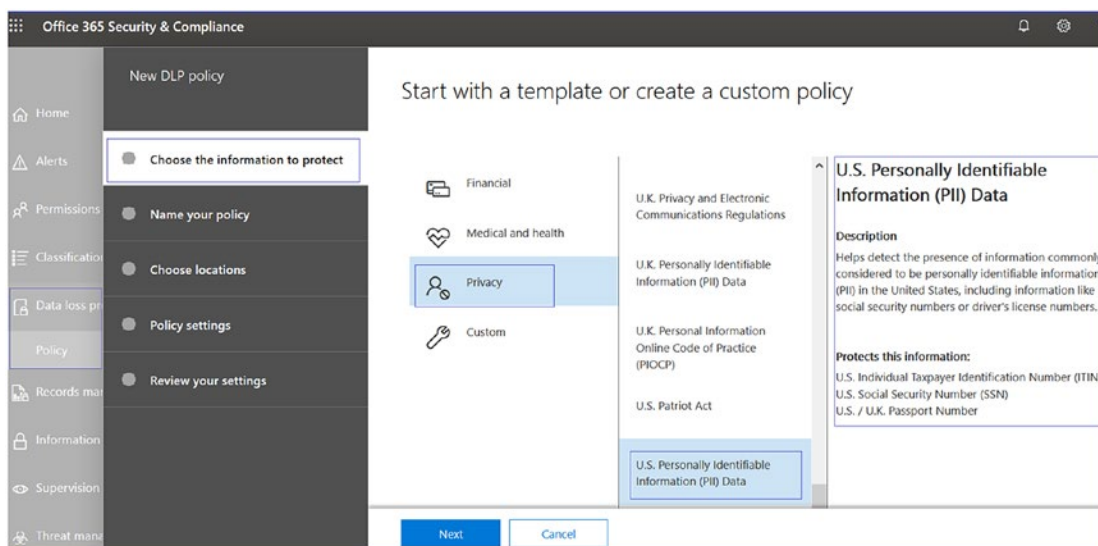


Figure 5-15. Choosing an available DLP template

3. On the next page, enter a name and description for the policy, and then click Next. Figure 5-16 shows the name given is U.S. Personally Identifiable Information (PII) Data- Bloguc Org, and the description identifies this policy correctly.

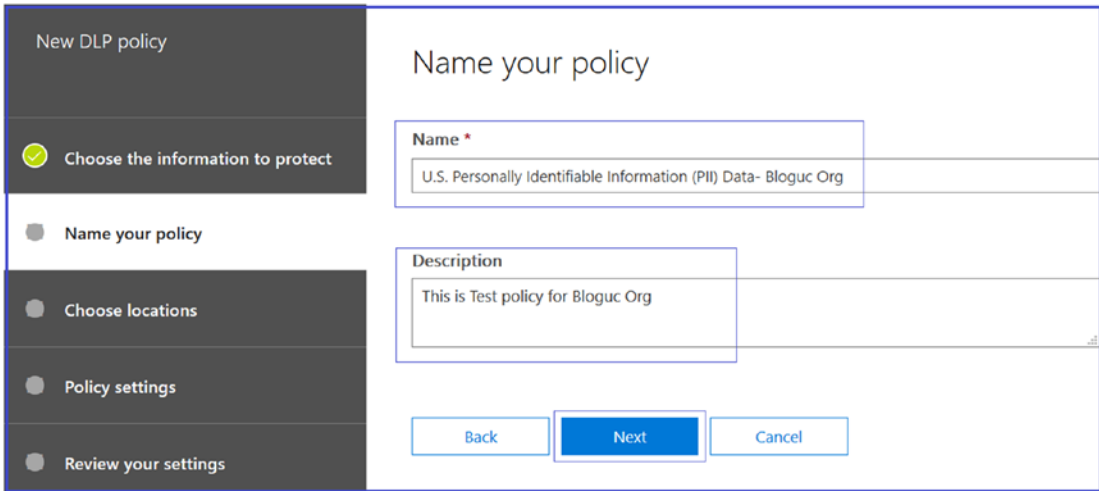


Figure 5-16. DLP policy name and description

4. On the next page, the Choose Locations tab, keep the default setting that includes all locations, or select Let Me Choose Specific Locations, and then click Next. For the example shown in Figure 5-17, the default selection that includes Exchange email, Teams chats, channel messages, and OneDrive and SharePoint documents is selected. If you have selected specific locations, select them for your DLP policy, and then click Next.

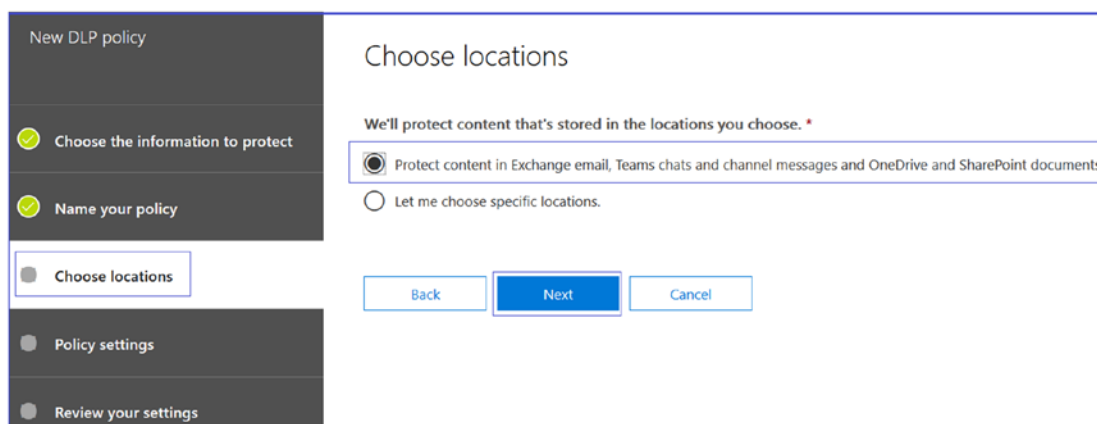


Figure 5-17. DLP policy locations

Note If you want to make sure documents that contain sensitive information are not shared inappropriately, make sure SharePoint sites and OneDrive accounts are turned on, along with Teams chat and channel messages. Channels in Microsoft Teams are strongly dependent on Exchange Online functionality. Make sure that the Exchange email location is also enabled for the policies that should be applied for the content of the channels [23a].

5. On the next page, the Policy Settings tab, under Customize The Type Of Content You Want To Protect, keep the simple default settings, or choose Use Advanced Settings, and then click Next. If you choose to use advanced settings, you can create or edit rules for your policy. For this example, shown in Figure 5-18, the default setting is retained to keep the policy simple.

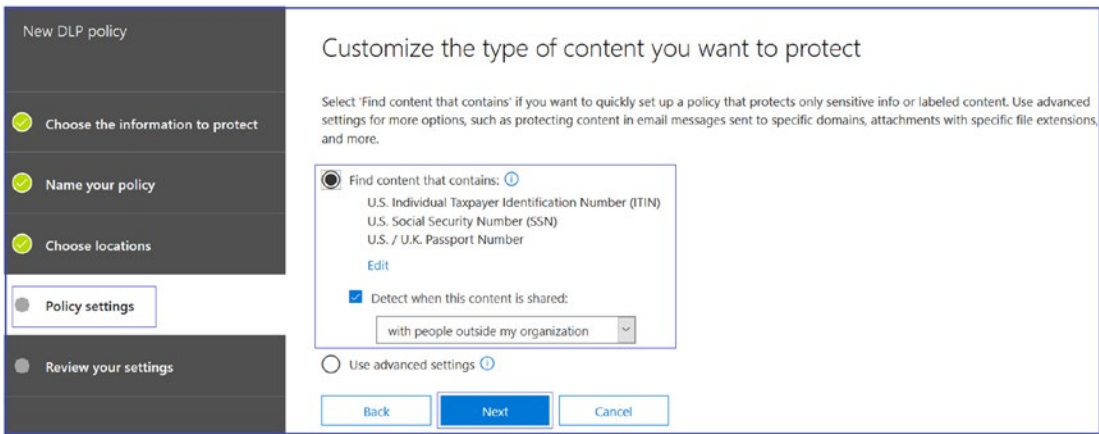


Figure 5-18. DLP policy settings

6. On the next page of the Policy Settings tab, under What Do You Want To Do If We Detect Sensitive Info?, review the settings. (Here’s where you can select to keep default policy tips and email notifications or customize them.) When you are done reviewing and editing the settings, click Next. For this example, all the default settings are retained, as shown in Figure 5-19.

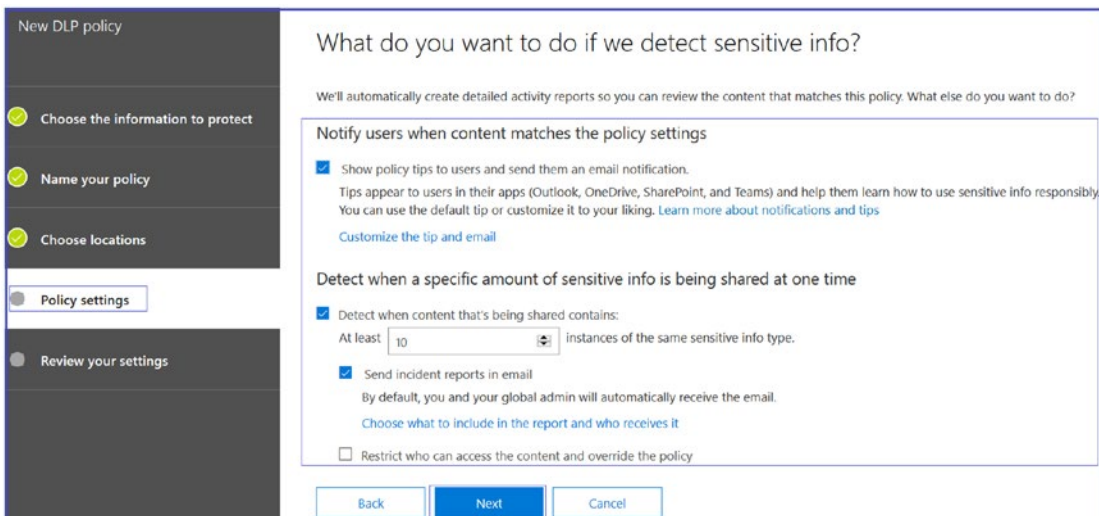


Figure 5-19. Policy settings for sensitive information

7. On the next page of the Policy Settings tab, under Do You Want To Turn On The Policy Or Test Things Out First?, select whether to turn the policy on, test it first, or keep it turned off for now, and then click Next. Testing the policy first before turning it on, as selected in Figure 5-20, is recommended.

New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- Policy settings
- Review your settings

Do you want to turn on the policy or test things out first?

Do you want to turn on the policy right away or test things out first?

Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

Yes, turn it on right away

I'd like to test it out first

Show policy tips while in test mode

No, keep it off. I'll turn it on later.

Back Next Cancel

Figure 5-20. Policy setting for testing

8. On the Review Your Settings tab, shown in Figure 5-21, review the settings for the new policy that you created. Select Edit to make changes if required. When you are finished making changes, click Create.

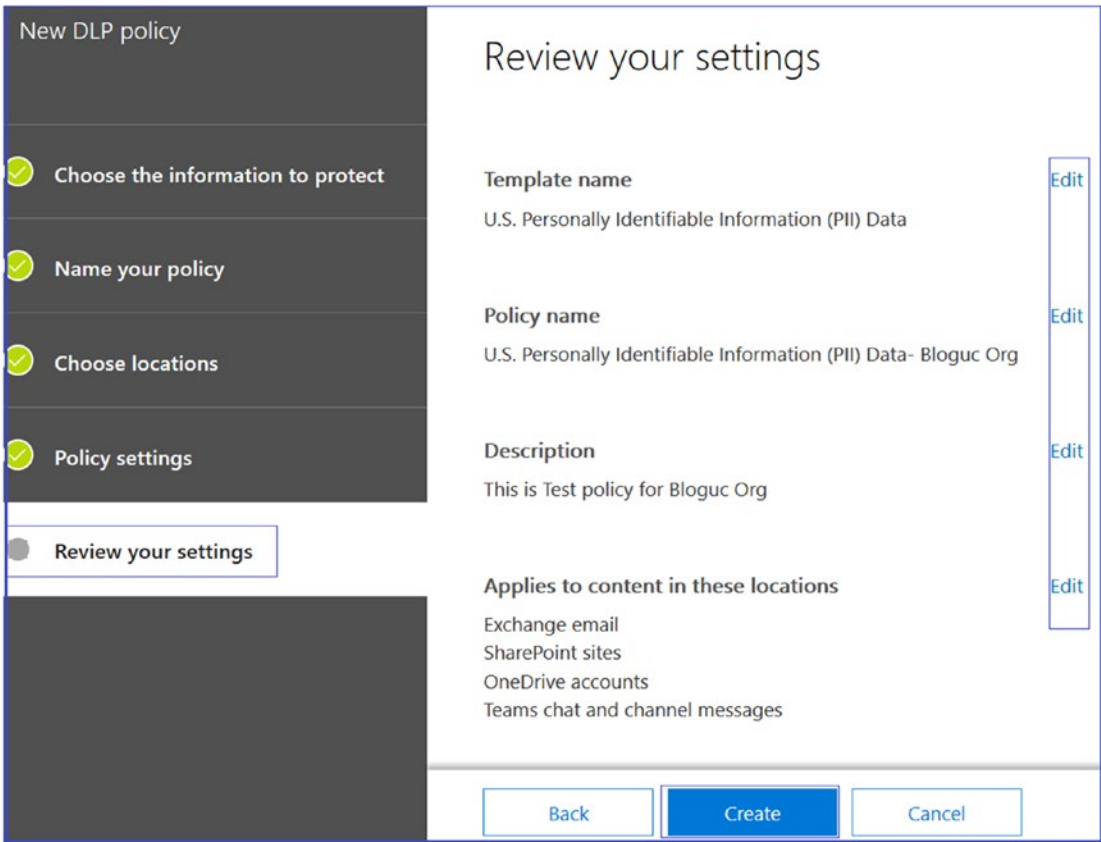


Figure 5-21. Reviewing settings

DLP policy could take some time to populate, so sometimes it takes up to an hour for your new policy to work. You can make changes in the policy that you created to customize the policy per your organization’s requirements.

Creating and Managing eDiscovery for Teams

From a manageability and content discovery perspective, Microsoft has provided some tools that Teams admins can use to retrieve information like who is creating content, monitoring, or reporting. Using Teams, you can discover the content through eDiscovery and put some users on a legal hold so that they cannot tamper with content that was created in Teams. For example, if User A is under litigation and he shared the information with an external user, then you as an admin have the workflow that will help to export the content and hand it out.

Create eDiscovery Workflows for Teams

You can access eDiscovery through the Office 365 Security & Compliance Center. The advanced eDiscovery workflow is available in Office 365 and Teams is one of the primary applications that can be used. In eDiscovery, you can search content that was created in Teams and content that was exchanged in conversation, including one-to-one chat, group chat, and channel chat. All these contents are discoverable to you as a Teams admin and security admins.

To use the eDiscovery search, first log in to <https://protection.office.com/> and then navigate to eDiscovery. Select eDiscovery or Advanced eDiscovery, as shown in Figure 5-22. Click + Create A Case to create a case for eDiscovery.

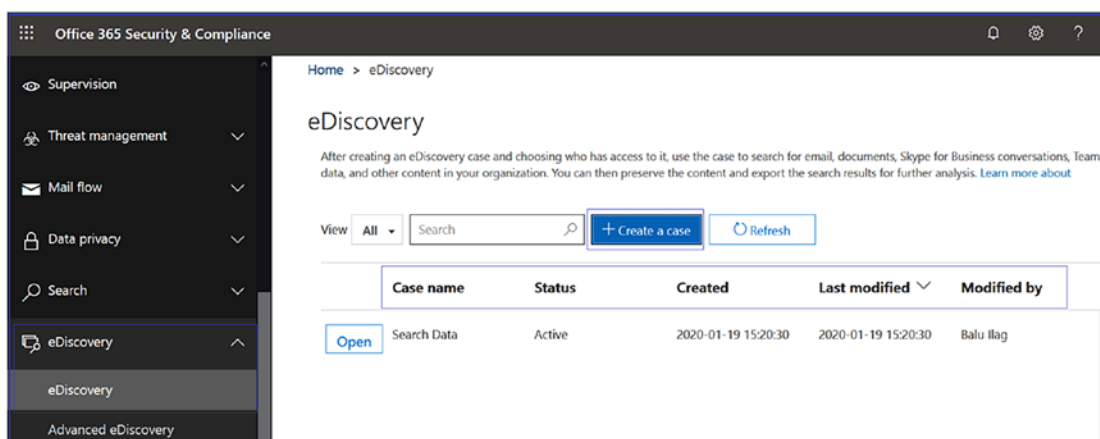


Figure 5-22. eDiscovery search

Microsoft has updated the eDiscovery search capability to show the threaded conversation view when a security admin searches in eDiscovery.

There is another feature, redaction, that Microsoft added in eDiscovery search, displayed in Figure 5-23. How does it work? Here is an example: You search some content that is required, and the requested content is one conversation. However, the search results show three threads of conversation. A security admin can activate redaction for the two conversation threads that are not required, so that only the required details are shared. You can manage the existing search cases that you have previously created under eDiscovery.

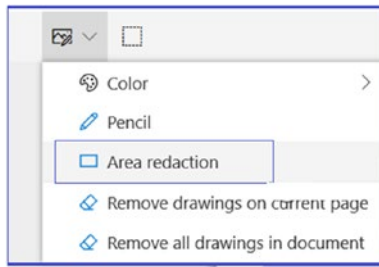


Figure 5-23. Redaction feature [22a]

Data Governance and Retention in Teams

Microsoft Teams is part of the Office 365 service that keeps everything secure. Additionally, it allows creation of retention policies.

Retention Policies for Teams

In Microsoft Teams, retention policies are very useful for retaining Teams or chat data, as well as defining deletion policies. For most organizations, the volume and complexity of data increases daily, including email to documents to instant messages, and many more. Efficiently managing or governing these data is very important because as a Teams admin, you should comply proactively with industry regulations and internal policies that require you to retain content for a minimum period of time. For example, the Sarbanes-Oxley (SOX) Act might require you to retain certain types of content for seven years. Teams is already certified by more than 42 regional or national and industry-specific regulations [22a].

This can also help reduce your risk in the event of litigation or a security breach by permanently deleting old content that you are no longer required to keep. Teams also helps your organization share knowledge effectively and be more responsive by ensuring that your users work only with content that is current and relevant to them.

Specific to the retention policy, it helps organizations either retain data for compliance (namely, preservation policy) for a specific period or remove data (namely, deletion policy) if it is considered a liability after a specific period. Retention policies are available in the Security & Compliance Center, and they work across the different workloads and data types, such as Exchange email, SharePoint document libraries, and OneDrive for Business files.

As you know, Teams chat conversations are persistent and retained by default in Exchange Online. With the addition of retention policies, administrators can configure retention policies (both preservation and deletion) in the Security & Compliance Center for Teams chat and channel messages.

Creating and Managing Retention Policies

Managing Retention Policies

You can manage retention policies using Office 365 Security & Compliance center, or you can use PowerShell. To manage Teams retention policies, log in to the Office 365 Security & Compliance Center and navigate to Information Governance. Select Retention, as shown in Figure 5-24.

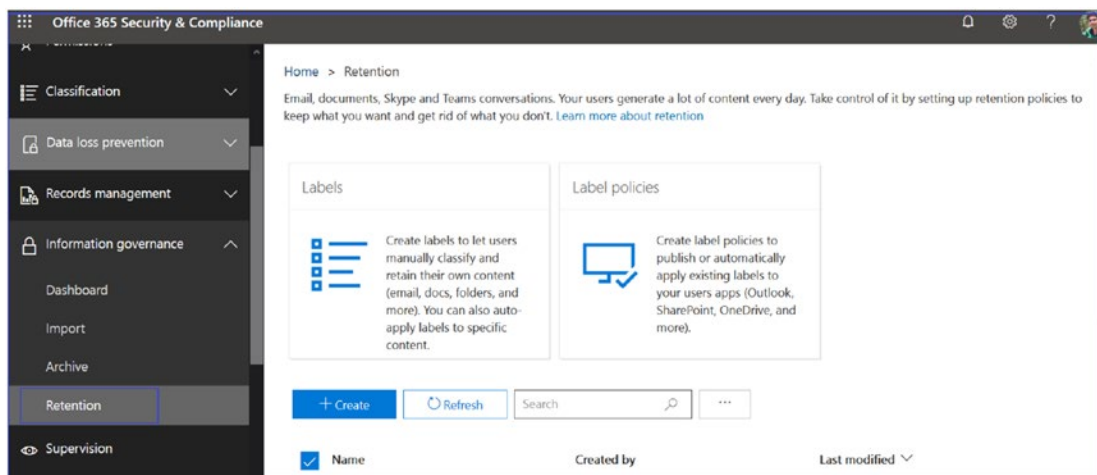


Figure 5-24. Retention policy

Microsoft Teams retention policies support different tasks, such as preservation, that allow an organization to keep Teams data for a specified duration and then do nothing. Another policy preserves and then deletes the Teams data. This kind of policy allows an organization to keep Teams data for a specified duration and then it will be deleted. In addition, there is another policy that allows deletion of Teams data after a specified duration.

So far, advanced retention policy doesn't support Teams chat and Teams channel message locations, but Microsoft might support advanced retention policy for Teams chat and channel messages in the future.

Creating Teams Retention Policy

As a Teams admin, you must know how to create retention policies for Teams private chats (one-to-one chat and group chat) and Teams channel messages. In many instances, organizations consider private chat data as more of a liability than channel messages, which are usually more project-related conversations. To create a retention policy, follow this procedure.

1. log in to Office 365 Security & Compliance Center (<https://protection.office.com/homepage>) and navigate to Information Governance. Select Retention and then click Create Policy.

Figure 5-25 shows settings for retention policy creation.

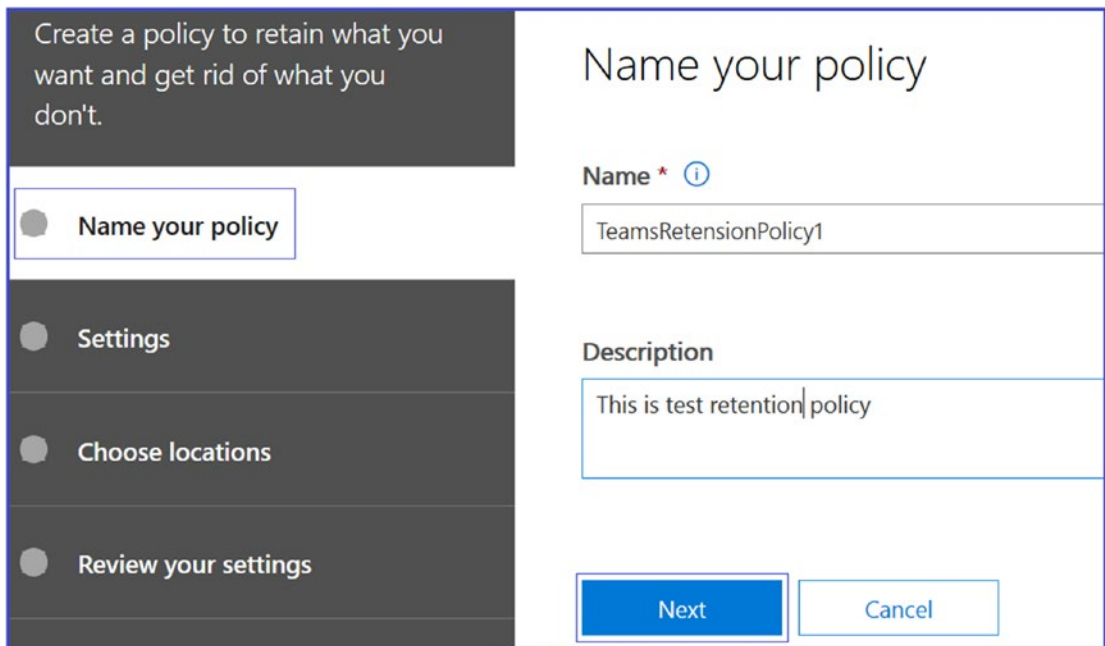


Figure 5-25. Creating a retention policy

2. Enter a meaningful name and description for the retention policy. Click Next.
3. On the Settings tab, define retention policies for these locations. Set how long you want to retain the content. For example, Figure 5-26 shows that the content will be retained for 7 years.

Figure 5-26. Retention policy settings and duration

4. Decide whether you want to delete the content after 7 years. Click Next.
5. On the Choose Locations tab, select the appropriate applications for retention, as shown in Figure 5-27.
6. Next, choose the locations for Teams and to which teams these settings will apply.
 - Turn on the Teams Channel Messages setting and choose for all teams or choose specific the teams.
 - Turn on Teams Chats and choose for all the users and or exclude users.
7. When you turn on Teams channel messages, you can specify teams to which this policy will apply. For example, for teams X, Y, and Z, the admin can set the deletion policies for 1 year (by selecting those teams individually) and apply a 3-year deletion policy to the rest of the teams. Click Next to review the settings.

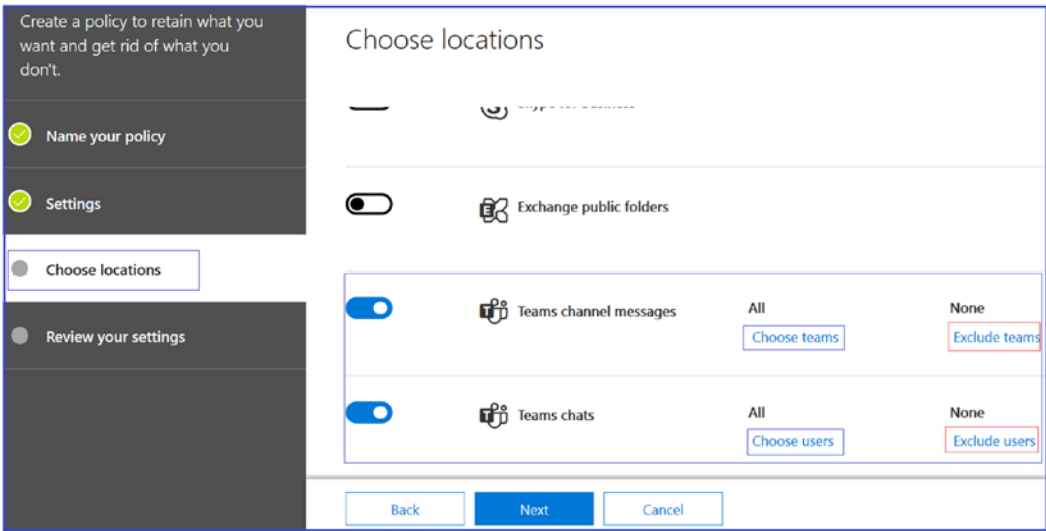


Figure 5-27. Choose location for retention

8. On the next tab, review all the settings and click Create This Policy, as shown in Figure 5-28.

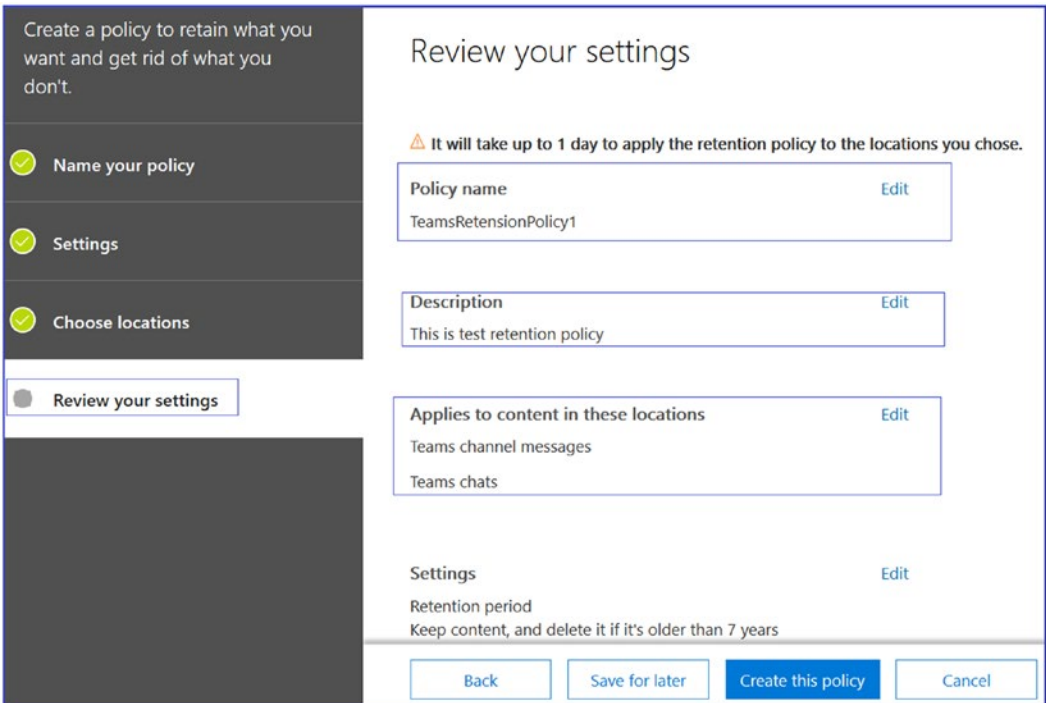


Figure 5-28. Reviewing the Retention policy

After policy creation you can see the policy created and its last modified date, as illustrated in Figure 5-29. In this example, Teams chats and Teams channel messages will be maintained for 7 years.

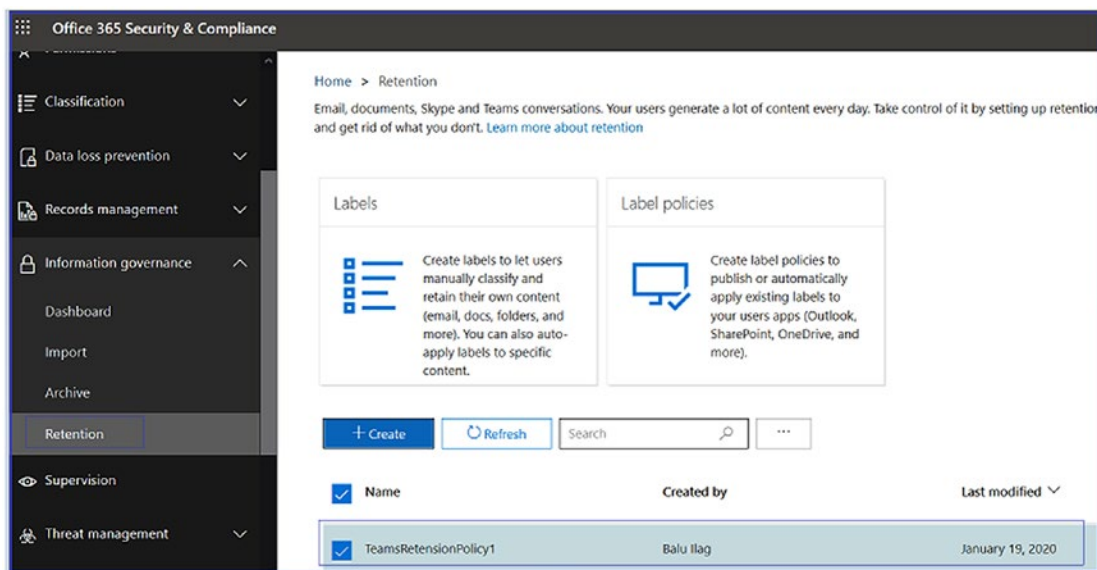


Figure 5-29. Retention policy created

Retention policies allow you to preserve your data for a specific amount of time and then delete the data after that period. Microsoft Teams supports retention policies as short as one day. Retention policies can be configured to retain data for a specific amount of time so that even if the user deletes the data, admins still have access to it. Another policy is to delete data, so if a user wants to delete data after specific period of time, then you will be able to do this.

You as a Teams admin can create a retention policy based on when the information is created, or you can create policies based on when information was last modified. Microsoft provides the flexibility to create retention policies based on the organization's requirements [99].

Managing Internal Risk Through Information Barrier in Teams

Managing internal risk is another important consideration. DLP prevents the compromise of sensitive information, but organizations are subject to different kinds of risk, such as IP theft, or content leaks, insider trading, and conflicts of interest.

Figure 5-30 shows several types of risk that organizations are subject to.



Figure 5-30. Risks that organizations face [22a]

One of the major tools that Teams uses to mitigate risk is the information barrier (IB). An IB is often called an ethical wall, a barrier in your organization created between different departments or internal units. For example, if you have groups of users that are not supposed to interact with other groups of users, you as a Teams or security admin can create segments and prevent these segments from talking to each other.

This setup is typically used in regulated industry, education, and financial sectors. Basically, IBs build logical boundaries to prevent communication between Group A and Group B. For example, investment bankers cannot find or communicate with financial advisors, but both groups can communicate with human resources (HR). The investment bankers cannot communicate with financial advisors because of potential influence issues. The Microsoft Teams solution is creation of IB segments, which ensure that you as an admin can put investment bankers in one segment and financial advisors in another segment. IB policies will prevent communication between the segments. Both segments, however, can communicate with the HR team without any barriers. This process is illustrated in Figure 5-31.

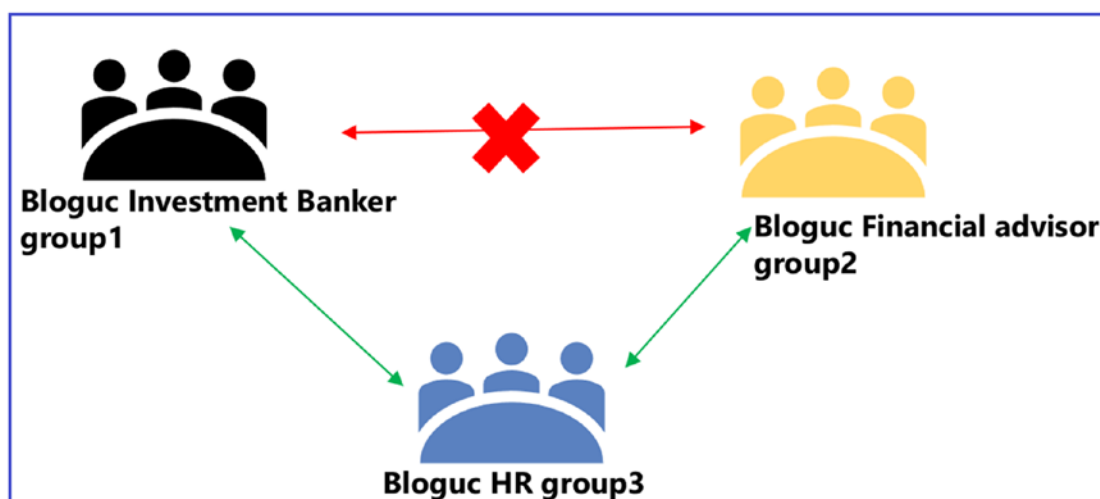


Figure 5-31. Information barriers between groups [22a]

Information Barrier Policies

IB policies allow you to control communication and collaboration in Microsoft 365 workloads between two groups of people. You can set IB policies to prevent a day trader from calling someone on the marketing team or to keep finance personnel working on confidential company information from receiving calls from certain groups within the organization. Perhaps the organization wants to allow a research team to call or chat online only with the product development team.

Who Can Set Up Information Barriers Policies?

The tenant admins, compliance administrator, or IB administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. IB policies can be defined to prevent or allow communications in Microsoft Teams. Such policies can prevent people from calling or chatting with those they shouldn't or enable people to communicate only with specific groups in Microsoft Teams. With IB policies in effect, whenever users who are covered by those policies attempt to communicate with others in Microsoft Teams, checks are performed to prevent (or allow) communication, as defined by IB policies [24a].

Note At present, IBs do not apply to email communications or to file sharing through SharePoint Online or OneDrive. In addition, IBs are independent from compliance boundaries.

Defining Information Barrier Policies

Before defining an IB policy, you as a Teams or security admin need to the prerequisites listed here.

1. Verify that you have the required licenses and permissions. IB is included in subscriptions such as Microsoft 365 E5, Office 365 E5, Office 365 Advanced Compliance, and Microsoft 365 E5 Information Protection and Compliance. Also, as a Teams admin you must have one of the following role permissions to define or edit IB policies:
 - Microsoft 365 global administrator
 - Office 365 global administrator
 - Compliance administrator
 - IB Compliance Management (this is a new role)
2. Validate that the directory includes data for the segmenting users. Make sure that your organization's structure is reflected in directory data. To do this, make sure that user account attributes, such as group membership, department name, and so on, are populated correctly in Azure AD (or Exchange Online).
3. Before you define your organization's first IB policy, you must enable scoped directory search in Microsoft Teams. Wait at least 24 hours after enabling scoped directory search before you set up or define IB policies.
4. To look up the status of a policy application, audit logging must be turned on. We recommend doing this before you begin to define segments or policies.

5. Before you define and apply IB policies, make sure no Exchange address book policies are in place. (IBs are based on address book policies, but the two kinds of policies are not interchangeable.)
6. As of this writing, IB policies are defined and managed in the Office 365 Security & Compliance Center using PowerShell commands. No GUI is available.
7. When your policies are in place, IBs can remove people from chat sessions they are not supposed to be in. This helps ensure your organization remains compliant with policies and regulations. Use the following procedure to enable IB policies to work as expected in Microsoft Teams [24b].

Defining an IB policy is a three-part process.

1. Segment the users in your organization by determining what policies are needed, then make a list of segments. Identify which attributes to use and then define segments in terms of policy filters.
2. Define the IB policies, but do not apply them yet. Select from two kinds: block or allow.
3. Apply the IB policies involving tasks like setting policies to active status, running the policy application, and viewing policy status.

There are many steps involved in defining IB policies, and they change frequently. Refer to the Microsoft official documentation at <https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?> for up-to-date information.

Creating and Managing Office 365 Group Classification

Microsoft Teams is built on Office 365 Groups. Office 365 Groups has multiple capabilities, and one of them is classification, which is often used in organizations to classify content. As an admin, you can determine and add information about the group purpose. For example, your organization decides to inform users what type of documents are stored within the Office 365 Group. This type of group functionality is called group classification. You as an admin can configure group classification so that when users in your organization create a group, they can choose a classification like, Standard, Internal, or Confidential.

Note Office 365 Group classifications do not exist by default. Admins will need to create the group classifications so that users can apply them when they create a group.

Enabling and Configuring Office 365 Group Classifications

Remember, group classification is not enabled by default. Before users can apply classifications to Office 365 Groups, you as an admin need to configure the classifications using Azure AD Windows PowerShell commands. First, install the latest AzureADPreview module using the following PowerShell commands [99].

- Remove any earlier version of AzureADPreview using this command

```
Uninstall-Module AzureADPreview
Uninstall-Module azuread
```

- Install the latest version of AzureADPreview using this command.

```
Install-Module AzureADPreview
```

To configure the classifications Standard, Internal, and Confidential, use the following command.

```
$Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq
"Group.Unified"}
if (!(($Setting=Get-AzureADDirectorySetting|Where {$_.TemplateId
-eq $Template.
Id})) {$Setting = $Template.CreateDirectorySetting}
$setting["ClassificationList"] = "Standard, Internal, Confidential"
```

As the next step, you must associate a description with each classification using the settings attribute ClassificationDescriptions, where classification should match the strings in the ClassificationList. For example, to add a description to the classifications Standard, Internal, and Confidential, run the following command.

```
$setting["ClassificationDescriptions"] = "Standard: General communication,
Internal: Company internal data, Confidential: Data that has regulatory
requirements"
```

To validate that the classification configuration is added correctly to the group, you need to run the `$Setting. Values` command.

To commit the setting to Azure AD and make sure the classifications can be applied by your users, you need to run this command.

```
Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
```

Note The classification settings update could take an hour before they are available for all users, so be patient after configuring the classification.

Configuring Classifications from Outlook and Teams Client

After enabling Office 365 Group classifications, you as an admin can assign the classification to a group from Outlook or Teams client. To do so, log in to Microsoft Teams client and select Teams. Select Join Or Create and then select appropriate the classification, as shown in Figure 5-32.

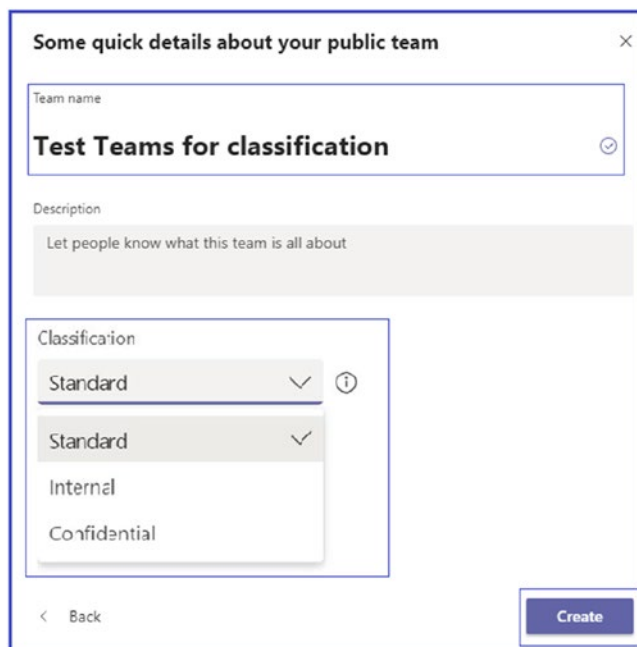


Figure 5-32. Classification options

You can also configure classifications on Office 365 Groups using Windows PowerShell. To set a classification to an Office 365 Group, you use the `Set-UnifiedGroup` command with the `-Classification` parameter. For example, to set a Confidential classification on the group `SecretData@bloguc.com`, run this command in Exchange Online PowerShell.

```
Set-UnifiedGroup "SecretData@bloguc.com" -Classification "Confidential"
```

You can also create a group and assign a classification during the group creation process. For example, to create a new private group named `HRDepartment@bloguc.com` with a classification of Internal, run the following cmdlet:

```
New-UnifiedGroup "HRDepartment@bloguc.com" -Classification "Internal"  
-AccessType "Private"
```

Creating and Managing Office 365 Group Expiration Policy That Applies to Associated Content

Microsoft Teams is built on Office 365 Groups and every team has Office 365 Groups associated with it. This means whenever a user creates a new team, an Office 365 Group is automatically provisioned. Therefore, as the number of teams grows, the Office 365 Group count automatically grows as well. As a Teams admin, you must manage these groups to control their expansion. In many cases, users create a team for a specific task, but after that task is completed, the team and Office 365 Group remain active but unused. For example, User A created a team for implementing Microsoft Identity Manager in Bloguc Organization. When the project ended, User A forgot to delete that project team. That means the Office 365 Groups and team content still exist. Such use cases will increase the Office 365 Group (and team) count, which adds to management overhead and eventually makes IT administration difficult.

To manage Office 365 Groups regardless of a team's association, you need a method to clean up the unused groups and simplify management. The best solution is to set a group expiration policy, which helps to remove unused groups from the directory system. The group expiration is turned off by default in Office 365. When you decide to implement group expiration, you need to enable the feature for your organization

tenants and specify an expiration period for the Office 365 Group. Once you set up group expiration, when the expiration date for a group approaches, an email notification is sent to the group owners (whoever created or was set as an owner of the group) to determine if group renewal is required for an additional period. If the group is not renewed, it will be deleted automatically [95].

Note If group expiration policy changes are made by an admin, the Office 365 expiration period will be recalculated for the groups.

Important When an Office 365 Group expires, all the group's associated content will be deleted, including Outlook, Planner, and SharePoint. However, there is an option to recover content for up to 30 days from the expiration date.

Note Renewal notifications are emailed to group owners 30 days, 15 days, and 1 day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Microsoft Teams, and PowerBI.

To configure the Office 365 Group expiration policy, perform these steps.

1. Log in to Azure Active Directory admin center (<https://aad.portal.azure.com/>) as a global administrator. In the left pane, select Azure Active Directory. Under Manage, select Groups, and then select Expiration to open the expiration settings page, shown in Figure 5-33.

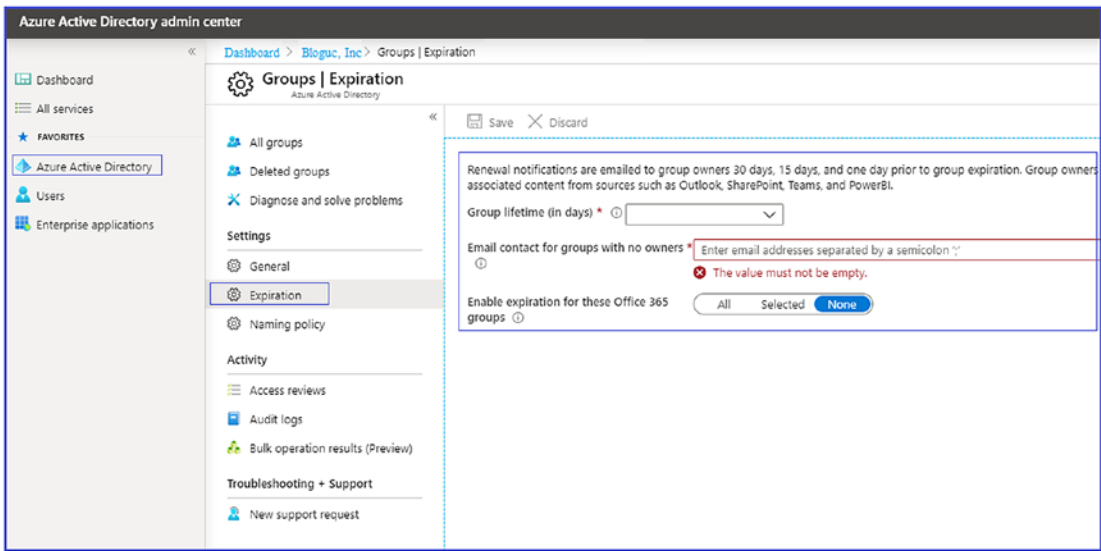


Figure 5-33. Group expiration settings page

2. On the Expiration page, you can specify several options.
 - *Group Lifetime (In Days):* This option sets the group lifetime in days with choices of 180, 365, or Custom. The Custom setting requires a lifetime of at least 30 days. The example in Figure 5-34 shows a setting of Custom and 90 days.
 - *Email Contact For Groups With No Owners:* Specify an email address where the renewal and expiration notifications should be sent when a group has no owner. If the group does not have an owner, the expiration emails will go to a specified admin. Figure 5-34 shows the contact email account for groups with no owner.
 - *Enable Expiration For These Office 365 Groups:* Select the Office 365 Groups for which you would like to configure this expiration policy. The options are All, for all the groups within your organization; Selected, for only specific groups; and None, which turns this off entirely. For this example, in Figure 5-34, the Selected option is chosen and the group Test is specified.

Note You should set the expiration policy for a test group first. Once this setting is properly tested, then you can enable expiration policy for the all the groups in your organization.

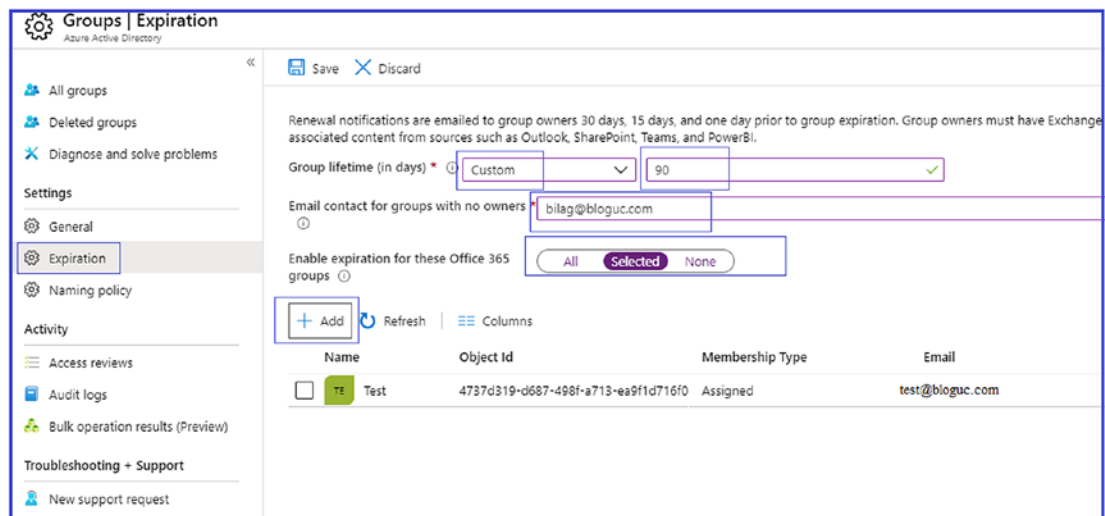


Figure 5-34. Group expiration settings

3. After finishing the configuration, click Save.

Remember that group expiration is a feature that is incorporated in an Azure AD Premium subscription. An Azure subscription license is necessary for the admins who are going to configure the settings and the members of the affected groups. Specific to the management aspect, you as a Teams admin (with Office 365 global admin group permission) can create, view, modify, or delete the Office 365 Groups expiration policy settings and users can renew or restore an Office 365 Group that they own.

How Group Expiration Works with the Retention Policy

When you as a security admin set up a retention policy in the Microsoft 365 Security & Compliance Center for groups, then the expiration policy works in association with retention policy. Once a group expires, the group's conversations in Outlook and files in SharePoint Online are kept in the retention container for the duration (number of days)

specified in the retention policy. The users will not see the group or its content after expiration, however. That's why a user must monitor the group expiration notification and act in a timely manner instead of losing control of their content [96].

How Group Owners Receive Expiration Notifications

Specific to the group expiration notification, when a group is about to expire, group owners will be notified via email, irrespective of how the group was created, whether through SharePoint, Planner, Teams, or any other Office 365 application. If the group was created via Teams, the group owner will receive a notification to renew through the activity section in the Microsoft Teams client. The group owner will receive the group expiration notification before 30 days, and if it is not renewed, an additional renewal email will be sent 15 days before the expiration. In the event the group is still not renewed, one more email notification will be sent the day before the expiration.

If no one renews the group before it expires, it will be automatically deleted, but the admins will still be able to restore the group within 30 days after the expiration date. It is important to understand that not every admin can restore the expired group, as specific permissions are required to restore a group: Global administrators, Group administrators, Partner Tier2 support, and Intune administrators can restore any deleted Office 365 Group.

Creating and Managing Office 365 Groups Naming Policy Applicable to Teams

When a user creates an Office 365 Group or Microsoft Teams team (which creates an Office 365 Group in the back end) for their professional use then the expectation is that they should use a meaningful name. Out of the box, users can use any name while creating a group, but if your organization requires a specific naming format, you as an admin can achieve this using a group naming policy that implements a consistent naming strategy for groups created by users. The naming policy will be able to help users identify the function of the group, membership, or the person who created the group. The policy is applied to groups that are created across all Office 365 apps, including Outlook, Teams, SharePoint, Planner, and Yammer. It applies for group names and group aliases, as well.

When creating a naming policy, you must be aware that the maximum group name length is 53 characters, including the prefixes and suffixes. Prefixes and suffixes can

contain special characters in the group name (and group alias), and if they contain special characters that are not allowed in the group name they will be removed and applied to the group alias. This will result in group prefixes and suffixes that will be different from the ones applied to the group alias. Finally, be aware that if you are using Yammer Office 365 connected groups, avoid using the following characters in your naming policy: @, #, [,], <, and >. If these characters are in the naming policy, regular Yammer users will not be able to create groups.

The Office 365 Group naming policy includes a prefix-suffix naming policy. You can use prefixes or suffixes to describe the naming convention of groups. For example, if you configure GRP as a prefix, then the Marketing group will be names GRP Marketing. Custom blocked words is another important features, as it allows an admin to specify a variety of words that will be blocked in groups created by users, such as CEO, CFO, Invoice, Billings, Payments, HR, and so on.

Working with Prefixes and Suffixes in a Group Naming Policy

Specific to the naming policy, prefixes and suffixes can either be fixed strings or user attributes. When using fixed strings, it is advised that an admin assign short strings that will help differentiate groups in the Global Address List (GAL). Some of the frequently used prefixes and suffixes are keywords such as, Ext_name, Int_name, Grp_Name, #Name, or _Name.

Using attributes, you can use attributes that can assist in identification of which user has created the group, like [Department], and where it was created from, like [Country]. For example, a naming policy of GRP [GroupName] [Department] will result in the following if the group is named My Group and the user's department is Marketing: GRP My Group Marketing. Attributes supported in Azure AD are [Department], [Company], [Office], [StateOrProvince], [CountryOrRegion], and [Title]. Unsupported user attributes are considered fixed strings (e.g., [postalCode]). Also, extension attributes and custom attributes are not supported. It's advisable to use attributes that have values filled in for all the users in your organization and not to use attributes that have longer values.

Creating and Managing Group Naming Policy in Office 365 Tenant

Naming policy provides a way to standardize Office 365 Groups naming, and it allows you to block certain names as well. You can configure naming policy using Azure AD admin center and Windows PowerShell. To create a naming policy, follow this procedure.

1. Log in to Azure Active Directory admin center (<https://aad.portal.azure.com/>) as a global administrator. In the left pane, select Azure Active Directory. Under Manage, select Groups. In the Settings section, select Naming Policy. Open the Group Naming Policy tab, shown in Figure 5-35.

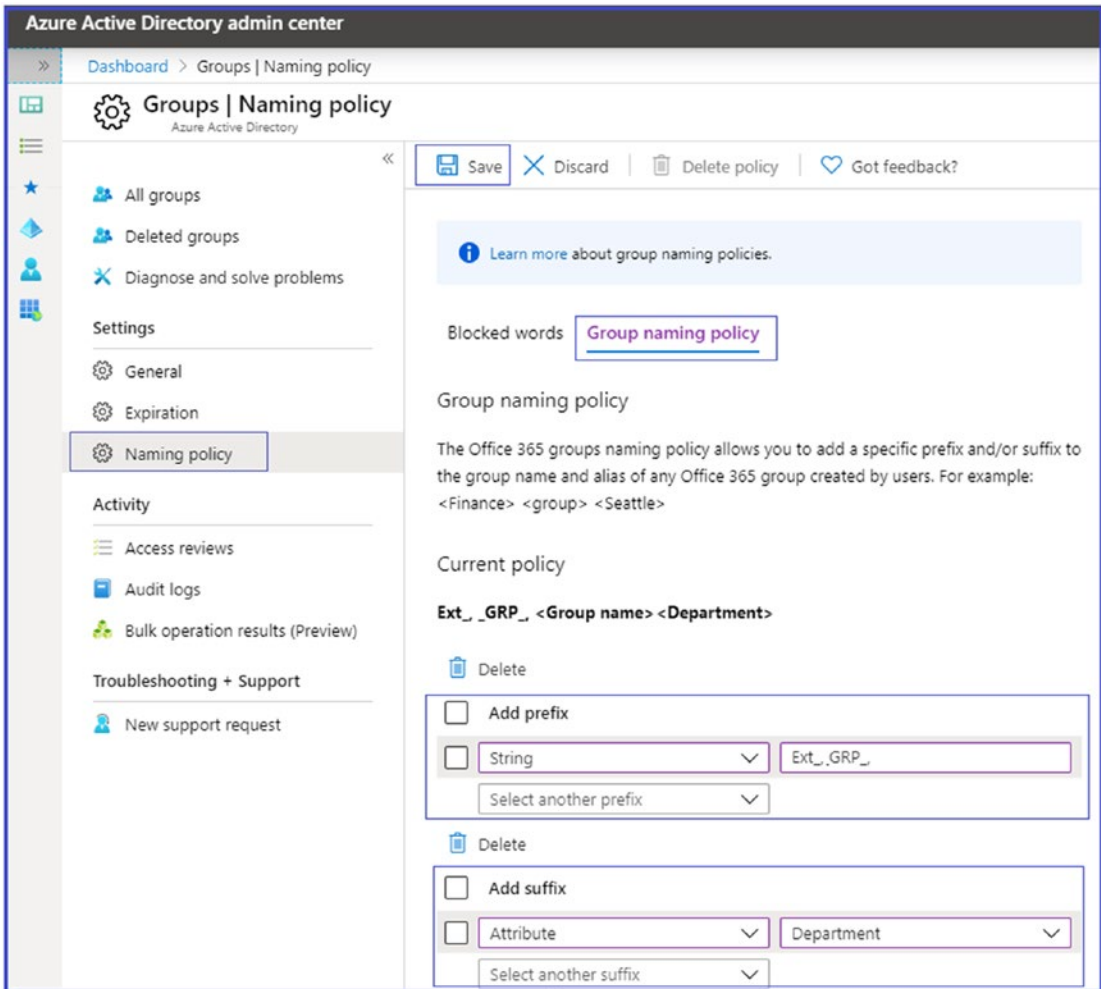


Figure 5-35. Creating a naming policy

2. In the Current Policy section, select whether you would like to require a prefix or suffix (or both) and select the appropriate check boxes. For either of these settings, choose between Attribute and String. Figure 5-35 shows the Ext_ and GRP_ prefixes and a Department suffix selected.

Creating Office 365 Groups Naming Policy Using Windows PowerShell with Azure AD Module

Before creating a new policy, you must check if any existing Office 365 Groups naming policy is available. Install latest Azure AD PowerShell module (if it is not already installed). Open Windows PowerShell as an administrator and connect to Azure AD, and then run this command.

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting |
where -Property DisplayName -Value "Group.Unified" -EQ).id
$Setting.Values
```

In the output, check the values for CustomBlockedWordsList, EnableMSStandardBlockedWords, and PrefixSuffixNamingRequirement.

Execute the next PowerShell command to create the naming policy in the existing PowerShell module that is connected to the Azure AD.

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting |
where -Property DisplayName -Value "Group.Unified" -EQ).id
```

Set the group name prefixes and suffixes; for example, the prefixes Ext_ and GRP_.

```
$Setting["PrefixSuffixNamingRequirement"] = "Ext_[GroupName]", "GRP_
[GroupName]"
```

To configure custom blocked words that you want to restrict— for example, Invoices, Payroll, and CEO—run this command.

```
$Setting["CustomBlockedWordsList"]="Invoices,Payroll,CEO"
```

You can modify the setting in the Azure AD directory by running this command.

```
Set-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where
-Property DisplayName -Value "Group.Unified" -EQ).id -DirectorySetting
$Setting
```

Managing Naming Policy

You can add or remove a naming policy using Azure AD. To add or remove a naming policy, log in to Azure AD and then open the Naming Policy page to add or modify the policy. If you are removing an existing policy, then it will ask for confirmation. Once you confirm the deletion, the naming policy is removed, along with all prefix-suffix naming policies and any custom blocked words.

Adding Custom Blocked Words Under Naming Policy

In a naming policy, custom blocked words are those users are not permitted to use when creating a group. You can also list several blocked words, which need to be separated by a comma. The blocked words check is done on the group name when it is entered by a user. For example, if a user enters CEO and Prefix_ as the naming policy, Prefix_CEO will fail. A substring search is not conducted, so that users can use common words like Pilot even if lot is a blocked word.

To add the a custom blocked word, log in to Azure AD. Under Manage, select Groups. In the Settings section, select Naming Policy, and then click the Blocked Words tab, shown in Figure 5-36.

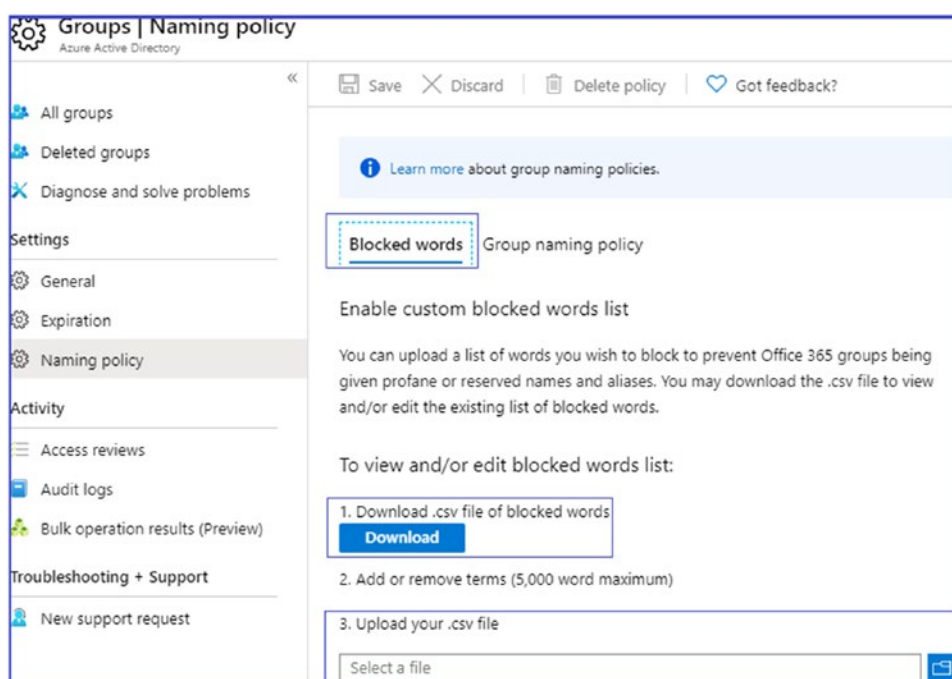


Figure 5-36. Custom blocked words

Summary

In summary Microsoft Teams is built on Office 365 Groups, which contains a set of tools to implement governance capabilities that any organization requires. In this chapter, you learned about the features you can use for Teams governance, including Teams identity management (including conditional access policies), DLP, eDiscovery, retention, and classification. You also learned how to set expiration policies and naming policies.

CHAPTER 6

Migration from Skype for Business (Lync) On-Premises and Online to Microsoft Teams

So far, you have learned about Microsoft Teams as an application, its service architecture, data storage, how the different Teams components communicate to each other, Teams policy management, Teams Phone System management, organization preparation and readiness including underlying network readiness, and so on. Now we'll look at what you need to understand to plan and execute a seamless migration from Skype for Business (Online and On-Premises) to Microsoft Teams. In this chapter, you will discover how Teams can benefit your organization, including IT and end users. You will also learn about the different migration paths and how to decide which path is appropriate for your organization and its considerations. In the end, you will be able to oversee an actual user migration through PowerShell commands and tools. We also cover best practices, guidance, and technical tips and tricks on your Teams migration journey.

Getting Ready for Microsoft Teams

As part of a user migration, a Teams admin needs to spread awareness about Teams and its features. While using Microsoft Teams, every user will have access to the chats, meetings, calls, content, apps, and workflow integration opportunity. Users will be able to participate in collaborative workspaces easily. Teams are a hub for teamwork and

provide the most robust platform to improve organizational productivity. Teams also bring provides a toolset for communication and collaboration, including persistent chat, calls, meetings, PSTN calling, and so on, that a team requires to be successful in its professional journey. It provides a integration of Office and third-party apps that users work with every day. Teams is part of Office 365; hence it includes enterprise-grade security and compliance with customization and management features.

First, understand why we need to consider migrating users from Skype for Business to Microsoft Teams. You might be aware that Microsoft will be retiring Skype for Business Online on July 31, 2021. Skype for Business Server is not affected by this announcement, but the organizations leveraging hybrid configurations will need to move Skype for Business Online users to Teams before the retirement date.

Ever since Microsoft launched Teams, it has continued to build new capabilities, functionalities, and features within Teams to enable end users to communicate and collaborate more effectively in new ways every single day. That is performance by design. It has positive effects on communication and collaboration in organizations. Teams functionality extends beyond what Skype for Business can do. Teams has advanced features and provides modern experiences. Teams combines chat, video, calling, collaboration, and app integration into a single, integrated hub that allows state-of-the-art, cross-platform, and mobile experiences. Teams provides better performance by design in terms of call and meeting quality, and it has reimaged a client built on a cloud infrastructure.

You, as an admin, must get ready for Teams, as it brings several benefits to businesses and end users. Organizations using Teams can make decisions more efficiently using enhanced meeting experiences with collaboration. In addition to that, they can engage in information sharing while keeping privacy a top priority using private channels within the project team. All Teams capabilities are available through a mobile client that boosts productivity as users can attend meetings and share documents even if they are not in the office.

From an end user perspective, they can join Teams meetings quickly with optimal audio and video quality. When users share the desktop in a meeting, Teams allows sharing control with user photos to quickly identify who has control. In a meeting, users can use a background blur feature so that they can work from anywhere. They can record meetings through cloud recording. In chat, users can use inline message translation, and emojis, and GIFs.

For the IT organization, Teams provides a single integrated platform for all productivity needs with end-to-end security and administrative controls. It brings a robust and highly available solution with improved performance and less downtime. In addition to that, it supports tabs, bots, and connectors for third-party integration.

Before user migration, admins must prepare the network environment, prepare the on-premises phone system SBC with Teams Direct Routing or Microsoft Phone System Calling Plan, create required call routing policies, test inbound and outbound phone calls, test meetings, and so on.

Understanding the Migration Path and Coexistence Modes

First you need to understand the terminology used in this section. User upgrades and user migration are used as synonyms. We will be using terms like Teams migration coexistence mode, Teams islands mode, Skype for Business with collaboration mode, Skype for Business with Teams collaboration mode, and meetings (meeting first) mode, and Teams only mode. The user coexistence modes shown in Figure 6-1 are used to determine both routing of incoming calls and chats and the app that is used by the user to initiate chats and calls or to schedule meetings. Each mode comes with a distinctive feature set.

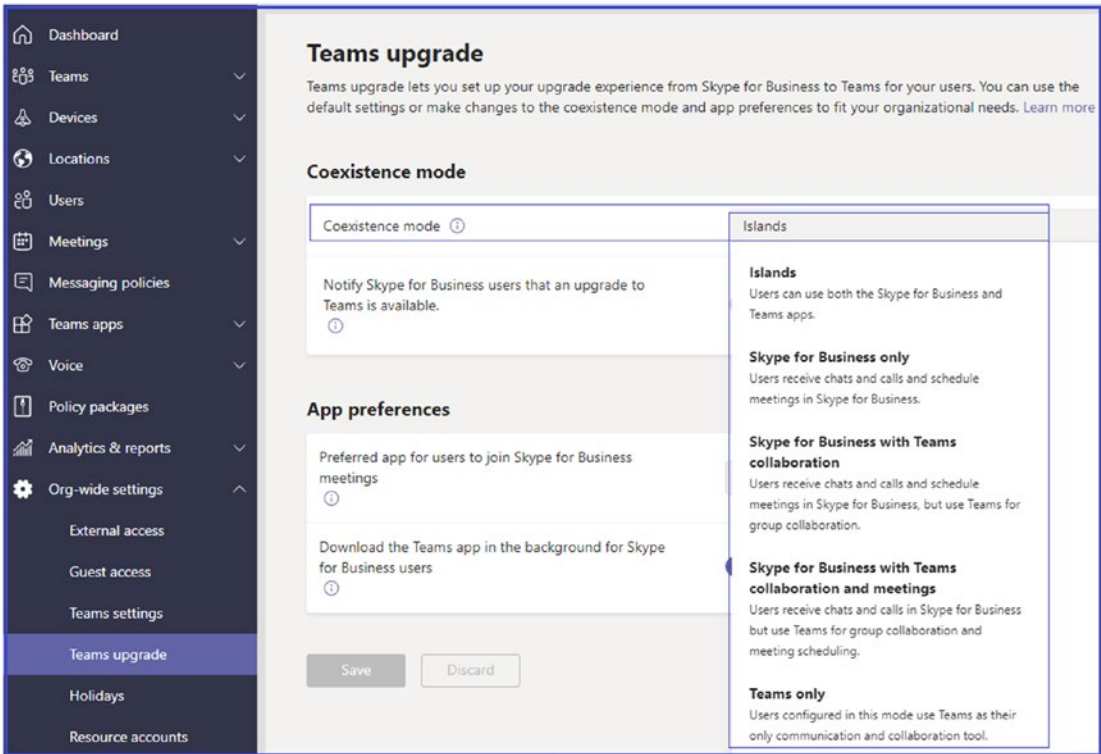


Figure 6-1. Teams upgrade coexistence mode list

When you think consider a Skype for Business to Teams migration, it’s not only about technology, but the users who are going to leverage Teams. Every organization’s success is dependent on users coming together, working effectively and efficiently. Without that collaboration, there will not be a strong business outcome. Teamwork is about people you are connecting with daily, why you are connecting, and how you are connecting. Teamwork means bringing all these pieces together.

Skype for Business is an excellent unified communication tool that provides chats, meeting, and calling capabilities. When you think about Microsoft Teams, it’s about full capabilities. Teams creates a hub for teamwork where users connect, communicate, and collaborate from within a single interface [64]. Figure 6-2 shows the difference between the two tools and their features.

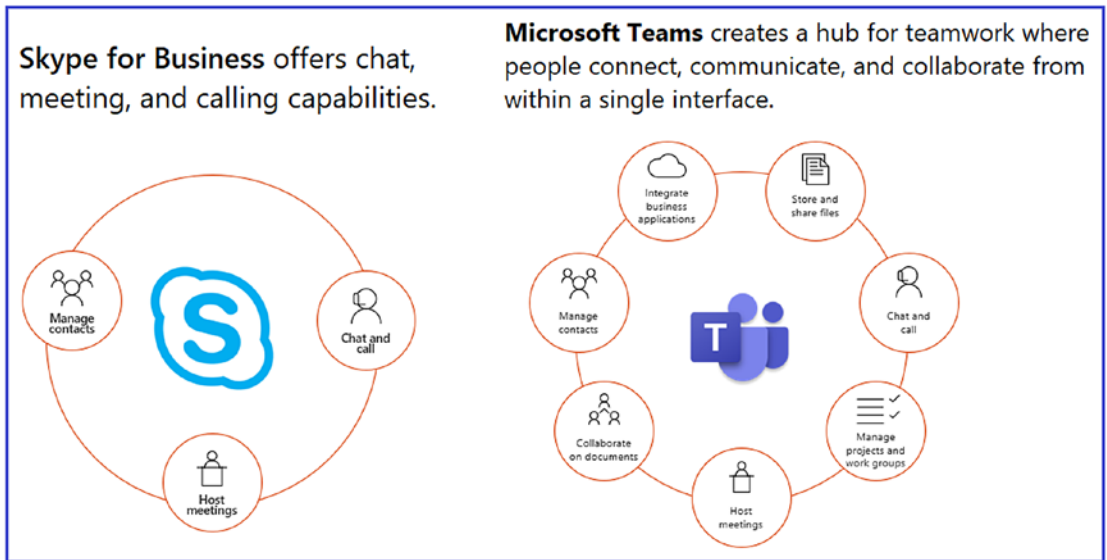


Figure 6-2. *Skype for Business and Teams features comparison [97]*

You need to have a focused plan based on user needs. Technical readiness and user readiness go together, and a solid operational plan is required for a consistent result. The completion of technical deployment includes network readiness and proof of concept (POC), then it will be ready for users. Communicating early and consistently will be the key. In addition to that, keep users updated on what back-end work is taking place during the Skype for Business to Teams migration.

Microsoft offers flexible approaches for enabling Teams alongside Skype for Business. The faster you get educate users about Teams and have them use whatever features they can, it will be useful for a smooth migration. The starting point might be an island mode where users work with Skype for Business and Teams side by side, with collaboration through Teams and calls, chats, and meetings through Teams.

Planning and Implementing a Successful Upgrade from Skype for Business to Teams

As a Teams admin, you need to understand that the adoption and technical migration efforts of Teams must go together. Without user adoption, you cannot be successful in a migration from Skype for Business to Teams.

As a starting point, you can create a team and channel to keep your project resources and team members in sync. For example, you can create a team underneath and you can

create a channel for project management, technical readiness, and user adoption. I have created a separate team and channel for the Bloguc Organization’s migration from Skype for Business to Teams.

After creating a team and channel, the next step in a successful migration is to identify the right team members working together toward migration work. You must have project sponsors like IT executives who sponsor the overall efforts, take accountability, and set the organization’s goals. You also need a project team with technical expertise who plans network readiness and executes the upgrade plan. You need a user change management team who drives adoption work, including end-user readiness. Additionally, it requires a project lead who will coordinate and report to the executive sponsor with an upgrade status.

Always start with a framework and scope the overall work and responsibilities. The user readiness team might indicate that in 30 days every user will have access on Teams with the phone system and every user will be upgraded to Teams only mode for chats, calls, meetings, Phone System, and content collaboration all in Teams, and the Skype for Business client will be used only to join Skype meetings. If the technical team comes back and says only pilot will roll out initially, then user migration might happen in phases after 60 days. This shows a complete disconnect, and that is why scoping with the timeline is particularly important. Throughout the preparation and migration work, check the Teams usage continually before and after the user upgrade [64].

Skype for Business to Microsoft Teams Upgrade Mode

Many coexistence modes are used to determine both routing of incoming calls and chats and the app that is used by the user to initiate chats and calls or to schedule meetings. Here is the list of coexistence modes considered in migration paths.

- *Island mode:* In this mode, users can use both the Skype for Business and Teams client apps for all the features these tools provide. In islands mode, each of the client applications operates as a separate island. Skype for Business talks to Skype for Business, and Teams talks to Teams. Users are expected to run both clients at all times. They can communicate natively in the client from which the communication was initiated.

- *Skype for Business only mode:* Using this mode, users receive chats, take calls, and schedule meetings in Skype for Business. Users continue to use only Skype for Business. They do not use Teams for chat, meeting, and calling capabilities; they do not use Teams for teams and channels. This mode can be used before starting a managed deployment of Teams to prevent users from starting to use Teams ahead user readiness. This can also be used to enable authenticated participation in Teams meetings for Skype for Business users, provided the users are licensed for Teams.
- *Skype for Business with Teams collaboration (Teams Collab) mode:* Using this Teams coexistence mode, users receive chats, handle calls, and schedule meetings in Skype for Business, but use Teams purely for the group collaboration. That means no chat, no calls, and no meetings in Teams. In this collaboration mode, Skype for Business remains unchanged for chat, calling, and meeting capabilities, and Teams is used for collaboration capabilities only, such as teams and channels, access to files in Office 365, and applications. This mode is a legitimate 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 mode:* Using this mode, users participate in chats and calls in Skype for Business, but use Teams for group collaboration and meeting scheduling.
- *Teams only mode:* This is the final stage, when Skype for Business users are ultimately migrated to Teams only. Users configured in this mode, with Teams as their only communication and collaboration tools, receive chats, handle calls, engage in content collaboration, and schedule meetings in the Teams app only. The Skype for Business client is used only to join Skype for Business only meetings.

These coexistence modes all have different feature sets and can be used based on your organization's needs and requirements.

Teams Upgrade Coexistence Modes Are Available as Deployment Path

When you plan to upgrade users to Teams, the starting point in all cases includes Skype for Business (On-Premises and Online) only mode, and the endpoint is always all users using Teams only mode. A planned deployment path is the most critical success factor in a Teams migration scenario.

User migration from Skype for Business to Teams is pretty straightforward, as it involves applying a few policies. Once the user is updated to Teams only mode, and Skype for Business is used only for meetings, users must use the Teams app for all kinds of communication. All routing automatically happens for chat, calling, meetings, external access (federation), and phone system (PSTN); the workload will be moved completely to Teams. However, if users are not ready for the upgrade because they haven't used Teams for any kind of communication and they are not familiar with Teams, you might not have success. Before migration, users must be familiar with Teams to have a successful adoption.

There are multiple considerations when you are deciding on an upgrade path, such as what the interoperability experience looks like. Make sure the feature overlap between Skype for Business and Teams is acceptable to users. You can either move all users at one time or by site or region, depending on what will work better for your organization. You might move collaboration features first, and then meetings and then the phone system (PSTN), you could move all features together. These are some of the decisions you, as Teams admin, must make before starting the migration.

- By default, users get the full side-by-side experience, which means Skype for Business and Microsoft Teams, both clients working, for chat, calling, and meetings. Skype for Business and Microsoft Teams do not work together in this scenario, and there will be no interoperability between these two clients.
- Another consideration is whether you want to move users to Teams with all features at once or first move meetings and then move users to Teams with phone system (PSTN), chat, calling, and so on. That decision will dictate the coexisting experience; for example, some users might be using Teams only mode while the rest of the users are using Skype for Business and Teams in island mode using one path.

- You also need to decide if your organization is ready for the default experience or an interoperability experience.
- The last thing you need to consider is how long you want the interoperability experience or the user upgrade duration to be.

After you make all these decisions, the next step is to choose an appropriate upgrade mode for your organization users. All the coexistence modes represent steps on the path toward Teams only mode, where all workload is handled in Teams and the legacy Skype for Business client launches only to join Skype for Business [64].

Teams Side-by-Side (Islands) Mode

Islands mode is the recommended path for Skype for Business Online and the on-premises organizations. However, because chat, calling, and meetings features are available in both Skype for Business and the Teams, some users might be confused by the feature overlap. Islands mode is enabled by default, so you, as a Teams admin, don't need to do anything special to configure this upgrade mode toward Teams path.

When you decide to choose islands mode, you should first introduce this to your users, so they are aware of the overlapping features, including chat, calling (VoIP), and meetings being enabled in both clients.

Remember, all the Teams upgrade coexistence modes can be configured per-user or tenant-wide using Teams admin center or Windows PowerShell by connecting to the Skype for Business Online PowerShell module.

How Overlapping Capabilities Work in Islands Mode

In this side-by-side mode, the Teams client and Skype for Business client don't have any interaction. Both clients will work independently for chat, calling, and meetings. Microsoft Teams will provide collaboration (content sharing), as well.

Again, awareness is the key here: You must drive the adoption program, notifying your users through email, perhaps arranging a large gathering, and providing as much information about Teams capabilities as you can to raise user awareness. Once the users know about the capabilities of Teams, and they are actively using Teams chat, calls, meetings, and collaboration features, the next step is to migrate users to Microsoft Teams only mode, assuming all back-end Teams work is completed, including, network readiness, Audio Conferencing and Phone System integration work. We recommend

running Teams only mode POC for at least 15 days and perhaps as long as a month, and then plan actual user migration on a site- or region-wide basis, or all at one time.

Remember, if you drive the Teams adoption properly and the majority of users begin using Teams gradually, then you can migrate all users to Teams at once without triggering coexistence modes. Figure 6-3 shows the overlapping features of Teams and Skype for Business [97].



Figure 6-3. Teams side-by-side with Skype for Business

Note Teams calling features are VoIP only until you move to the Teams only mode.

Features Available in Islands Mode

In the islands coexistence mode, users can run both applications with all features available. Specific to the calling and chat feature users will use these features separately in both clients, as described here.

- All users in islands mode can receive chats and calls in the same client as the one used by the originator. That means Skype for Business (SfB) users communicate with Skype for Business users and Microsoft Teams users communicate with Microsoft Teams users for chat, calls, and meetings (SfB <-> SfB and Teams <-> Teams).
- Users can initiate calls and chats from either client and the receiver receives it on the same type of client (SfB <-> SfB and Teams <-> Teams).

- Another important overlap feature is real-time presence status. Both of the clients have separate presence status, and they cannot share their presence status.
- There will be no interoperability between SfB and Teams client for calling, chat, presence, and meetings.
- For external access (federation), chat and calls land in the SfB client only.
- Phone System (PSTN) calls (inbound and outbound) land in the SfB client only.

There are some features specific to meetings.

- Online meeting scheduling is available on Microsoft Teams as well as Skype for Business on both the clients.
- In island mode, will see the Outlook meeting add-ins for the Teams as well as Skype for Business clients.
- End users can join meetings from the respective clients. Teams meetings are joined via the Teams client and SfB meetings are joined via the SfB client. There are no cross-meeting joins.

There are some issues to be aware of when using islands coexistence mode.

- Because both the Teams and SfB client features overlap for chat, calls, and meetings, users have to use the SfB client for SfB meetings and the Teams client for Teams meetings. Chats and calls will land on the originating clients. There is no interoperability between these two clients (until Teams users are moved to Teams only mode). For example, If the user Balu sends chat messages using SfB to the user Chanda, the same chat message will land on Chanda's SfB client. If the user Balu sends a chat message through a Teams client, then it will land on Chanda's Teams client. If Chanda is not running Teams client, then she will receive a missed notification after some time as the default behavior. For meetings, scheduling and joining is available in both clients (SfB <-> SfB and Teams <-> Teams).

- User migration at all once by region or site is the best option for an optimal user experience and simplified user adoption. I would recommend preparing the environment properly with network readiness and implementing Phone System (PSTN) integration through Direct Routing, voice policies, dial plans, or choose a Phone System Calling Plan so that you can move all your users at once. Large, complex organizations might have to run POC, however, and choose the region or site approach as per the organization and the deployment complexity involved.
- Chat messages and calls from federated users will be received on the Skype for Business client until the users move to Teams only mode.
- Phone System (PSTN) calling capabilities will only be available when users move to Teams only mode. Islands mode Teams users cannot use PSTN calling in the Teams client; it has to be in the SfB client only.
- Skype dominates an additional but essential consideration for the microphone and speaker device controls, as the Human Interface Device (HID) control for the Skype for Business client is used until the users migrate to Teams only mode.
- The last consideration is conference and meeting room devices, which must be upgraded or replaced or onboarded on Teams before the user migration so that when users are migrated to Teams, they can use a meeting room to join or host Teams meetings [64].

Some considerations have to be taken into account for Skype for Business Online organizations and some for Skype for Business On-Premises organizations, as enumerated next.

Considerations for Skype for Business Online Organizations

1. For Skype for Business Online, users must synchronize their on-premises AD users (if any) to Azure AD unless all users attributes are available in the online organization. The msRTCSIP attributes from on-premise AD must have been synced to Azure AD using Azure AD connect or another method. Skype for Business doesn't know about Microsoft Teams when a user enables Teams by activating its license.

When the Teams license is enabled for the user, it first determines if this user is already enabled for Skype for Business by looking at the msRTCSIP attributes. If a user is not already enabled for Skype for Business, then the Teams service will create a shadow account for the user for Skype for Business Online, which is going to be used as a gateway between online and on-premises conversations.

2. Microsoft Teams is a cloud-based service application, so the subscription license must be assigned to use Teams features. Teams service is part of the Office 365 suite with E1, E3, plus add-ons licenses for Phone Systems Audio Conferencing, or full E5 licenses with Phone System and Audio Conferencing as applicable.
3. Microsoft Teams does have prerequisites. All the corporate network locations from which users are accessing Office 365 services (Teams) must have Internet access, so that they can connect to Office 365 services for web (signaling) traffic. In addition, you must ensure that UDP ports 3478 through 3481 and IP subnets (13.107.64.0/18 and 52.112.0.0/14) are opened for Teams media traffic in all locations.
4. Additionally, implement QoS, split-tunnel VPN for the Teams audio/video call, conferencing, and desktop sharing scenarios. Refer to Chapter 3 for network readiness, QoS, and VPN split tunneling implementation.

Considerations for Skype for Business On-Premises Organizations

1. Using Skype for Business On-Premises only, you cannot move or upgrade users to Teams only mode. You must enable Skype for Business Hybrid first, which is required to start moving users to Teams only mode. As part of the hybrid configuration, you must sync all msRTCSIP attributes from on-premises Active Directory Domain Services (ADDS) to Online in Azure AD. Refer to the Microsoft documentation at <https://docs.microsoft.com/en-us/skypeforbusiness/hybrid/configure-federation-with-skype-for-business-online> on enabling a Skype for Business Hybrid configuration.

Note Users with Skype for Business On-Premises could use Teams, but they cannot be in Teams only mode.

2. If Skype for Business On-Premises users are enabled with enterprise voice, then you must have an enterprise license such as E3 with add-on licenses for Phone System and Audio Conferencing or E5 with an Audio Conferencing license. Without a proper license you cannot migrate users from Skype for Business to Microsoft Teams only mode.
3. Another consideration is the Skype for Business On-Premises user will not have interoperability, so there will be no external access (federation) from their Teams client (they must use the Skype for Business client for external access).
4. As a prerequisite for Microsoft Teams, all the corporate network locations from which users are accessing Office 365 services (Teams) must have Internet access, so they can connect to Office 365 services for web (signaling) traffic. In addition, ensure that UDP ports 3478 through 3481 and IP subnets (13.107.64.0/18 and 52.112.0.0/14) are opened for Teams media traffic in all locations.
5. Additionally, implement QoS and split-tunnel VPN for the Teams audio/video call, conferencing, and desktop sharing scenarios. Refer to Chapter 3 for network readiness and QoS and VPN split tunneling implementation.

Configuring Coexistence (Migration) Mode

As part of Skype for Business to Teams migration, as an admin you need to configure the coexistence mode for your tenant organization as well as individual users. You can select the same coexistence mode for all users and upgrade to Microsoft Teams all at once, or you could migrate a group of users from the same region or site, configuring different coexistence modes for different groups of users.

To set upgrade coexistence mode for all users using Teams admin center, follow this procedure.

1. Log in to Teams admin center, and navigate to Org-wide Settings. Select Teams Upgrade.
2. On the Teams Upgrade page, from the Coexistence Mode options, select one of the following coexistence modes for your organization, as shown in Figure 6-4.
 - Islands
 - Skype for Business only
 - Skype for Business with Teams collaboration
 - Skype for Business with Teams collaboration and meetings
 - Teams only

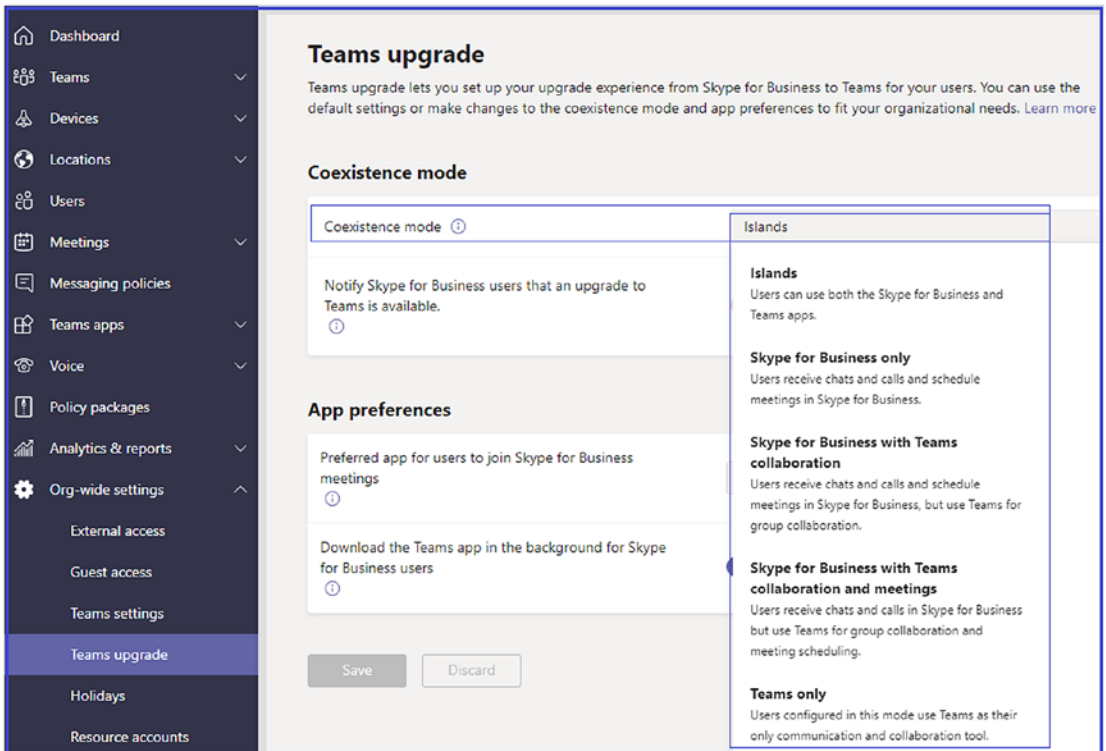


Figure 6-4. Teams coexistence modes

CHAPTER 6 MIGRATION FROM SKYPE FOR BUSINESS (LYNC) ON-PREMISES AND ONLINE TO MICROSOFT TEAMS

3. You can then enable Notify Skype For Business Users That An Upgrade To Teams Is Available when not selecting Teams only mode.
4. On the same Teams Upgrade page, you can set the Preferred App For Users To Join Skype For Business Meetings option (Skype Meetings App or Skype for Business), and you can also enable the Download The Teams App In The Background For Skype For Business Users option.
5. Finally, click Save to commit your changes.

You, as an admin, can select the Teams coexistence mode for an individual by following these steps.

1. Log in to Microsoft Teams admin center and navigate to Users. Find and select the user for whom you would like to set the upgrade options.
2. On the User page, on the Account tab, under Teams Upgrade, click Edit. On the Teams Upgrade page, select one of the options for the selected user, Use Org-wide Settings, and choose one of these upgrade options:
 - Islands
 - Skype for Business only
 - Skype for Business with Teams collaboration
 - Skype for Business with Teams collaboration and meetings
 - Teams only
3. Click Apply. 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. To do so, turn on the Notify The Skype For Business User option.
4. Finally, click Apply to commit the changes.

As an admin, you have the leverage to set the upgrade option using Windows PowerShell. To manage the transition from Skype for Business to Teams, you can use the `Grant-CsTeamsUpgradePolicy` command. This allows us to apply `TeamsUpgradePolicy` to individual users or to configure the default settings for an entire organization. For example, to configure the user `bilag@bloguc.com` to Teams in islands mode and to notify the user, run the following PowerShell command:

```
Grant-CsTeamsUpgradePolicy -PolicyName IslandsWithNotify -Identity "bilag@bloguc.com"
```

To configure a `TeamsOnly` policy for the entire organization, run the following command.

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

Migrating Users from Skype for Business Online (CCE) and On-Premises to Microsoft Teams (Teams Only Mode)

The Skype for Business to Microsoft Teams migration process is a three-step process at a high level.

1. Run the pilot; this allows validation of both technical and user readiness. It also allows this to be a formal effort with a defined test plan and clear go/no-go goals. You can then include a good representation of your user base.
2. Plan for coexisting, running Skype for Business and Teams together in your environment using several upgrade approaches (modes) to meet your organization's needs
3. Finally, perform the upgrade by moving users to Teams only mode. You can plan for a phased approach that enables you to pause or mitigate if needed. Maintain momentum once you begin to eliminate having users in too many modes [64].

As part of the user migration, each on-premises user must first move to Skype for Business Online using the command `Move-CsUser` and then execute the `Grant-CsTeamsUpgradePolicy` command with the policy name `UpgradeToTeams`. When you migrate users in a two-step process, first move users to Skype for Business Online. Then granting the upgrade policy does move users' meetings first to Skype for Business Online, and then they are converted to a Teams meeting URL.

You can do this as a one-step process using the `Move-CsUser` PowerShell command. You can use the switch `-MoveToTeams`, but doing so requires Skype for Business Server 2019 or Skype for Business 2015 with Cumulative Updates 8 (CU8). When you migrate the user in this one-step process using the `-MoveToTeams` switch, the users' calendar meetings will be moved and converted directly to a Teams meeting URL. Next we need to explain each scenario for user migration.

User Migration from Skype for Business Online to Teams Only Mode with or without Calling Plan

As a starting point, make sure user identity is available in Azure AD, specifically the `msRTCSIP` attribute should either be synced from On-Premises AD or created in Online. In this scenario, there is no Skype for Business On-Premises deployment.

The next step is to enable a user for appropriate licenses, including a Teams license and add-on licenses, and then deploy the Teams client to all the users' computers in your organization that are using Skype for Business. Then notify the users that Teams is available for them to use. To do so, in Teams admin center access **Teams > Org-wide Settings > Teams Upgrade > Coexistence mode**. Turn on the **Notify Skype For Business Users That An Upgrade To Teams Is Available** option. You can migrate Skype for Business Online users to Teams using the Teams admin center or Windows PowerShell.

Using Teams Admin Center

Log in to the Teams admin center and then navigate to **Org-wide Settings**. Select **Teams Upgrade**, and on the **Teams Upgrade** page, under **Coexistence Mode**, select the desired coexistence mode and turn on the **Notify Skype For Business Users That An Upgrade To Teams Is Available** option, as shown in [Figure 6-5](#).

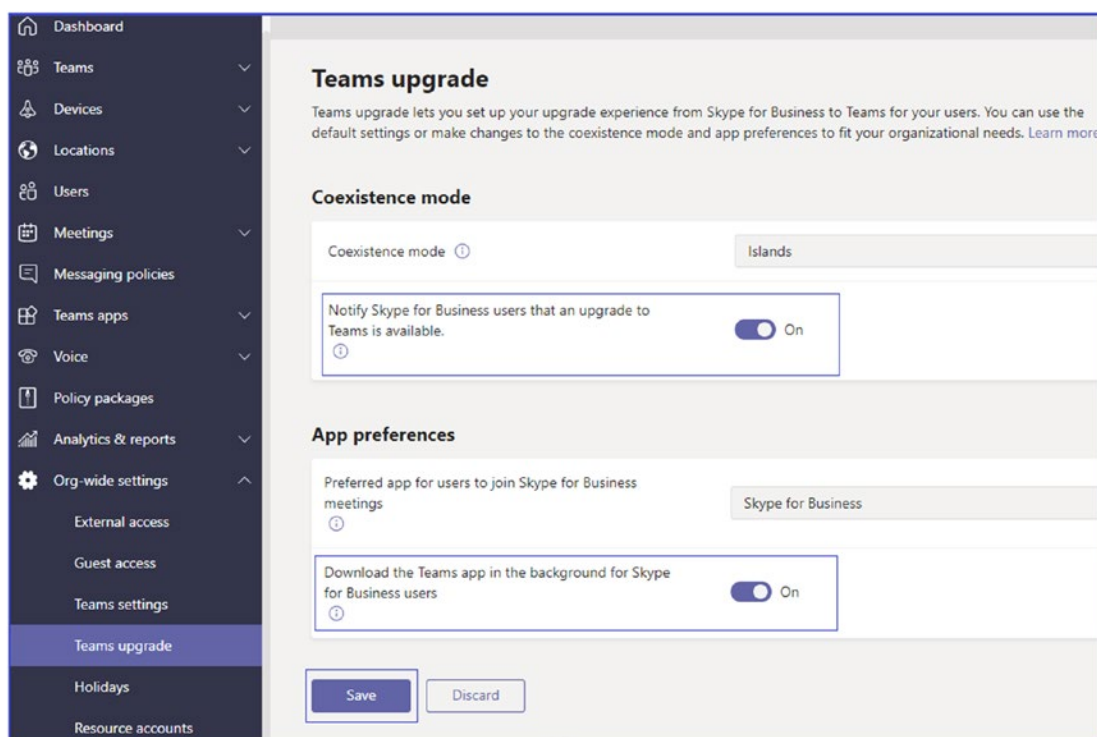


Figure 6-5. Upgrade notification

Using Windows PowerShell

To handle the migration in Windows PowerShell, run the following command.

```
Grant-CsTeamsUpgradePolicy -TeamsOnly IslandsWithNotify -Global
```

Organization-wide, you can enable all users. In Teams admin center, navigate to Teams ► Org-wide Settings ► Teams Upgrade ► Coexistence Mode, and change from Islands to Teams Only. To use PowerShell, use the following command.

```
Grant-CsTeamsUpgradePolicy -TeamsOnly UpgradeToTeams -Global
```

This assumes that the user doesn't have a voice routing policy.

Note In Skype for Business only, you can enable users directly to Teams only mode by selecting the coexisting mode as Teams only.

User Migration from Skype for Business Online Users with Cloud Connector Edition

In the Cloud Connector Edition (CCE) scenario, all the users are purely online or Azure AD synced. In this deployment type, there is no Skype for Business On-Premises footprint. All the users are deployed with CCE for voice, including PSTN.

In the CCE scenario, as part of provisioning, first assign the Teams license and Phone System license, and then deploy the Teams client to all users or groups of users in your organization who are using Skype for Business today.

The next step is to configure Teams Direct Routing or port existing phone numbers to Microsoft Phone Systems. Number porting will create an outage for the user while numbers are moved to Microsoft Teams, so plan number porting wisely.

Note Microsoft provided a Phone System Calling Plan that is not available in all regions. First, check the Calling Plan availability in your location by visiting this link: <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>. Once you decide and implement the Phone System Calling Plan or Phone System Direct Routing, then plan user notification.

Next, notify the users in your tenant that Teams is available for them using Teams admin center and PowerShell. In Teams admin center, navigate to Teams ► Org-wide Settings ► Teams Upgrade ► Coexistence Mode. Turn on the Notify Skype For Business Users That An Upgrade To Teams Is available option. Using PowerShell, run the following command.

```
Grant-CsTeamsUpgradePolicy -TeamsOnly IslandsWithNotify -Global
```

Finally, enable the tenant-wide setting to coexistence mode as Teams only using Teams admin center and PowerShell. In Teams admin center, navigate to Teams ► Org-wide Settings ► Teams Upgrade ► Coexistence Mode from islands mode to Teams only. Using PowerShell you can run this command.

```
Grant-CsTeamsUpgradePolicy -TeamsOnly UpgradeToTeams -Global
```

After configuration, you can assign the phone number to the user or configure the SBC to route the phone numbers for the user to Teams.

User Migration from Skype for Business On-Premises with Enterprise Voice to Teams Only with Direct Routing

The process for the on-premises users who are enabled for enterprise voice is similar to the Skype for Business Online and CCE scenario. The user must be synchronized with Azure AD for the msRTCSIP attribute. The Skype for Business On-Premises environment must be configured for a hybrid with a split domain in place. This means the same domain will be available in On-Premises as well as Online.

Users can be in any coexistence mode except Teams only. First, check the existing configuration using the following PowerShell command, and check that the user is enabled on-premises with a Direct Inward Dial (DID) number assigned.

```
Get-CsOnlineUser bilag@bloguc.com | Select Display*,*interp*,*voice* | fl
```

As part of user provisioning, the user must have the required license assigned, such as E1/E3 plus add-on licenses for Phone System and Audio Conferencing, or E5 with the Phone System and Audio Conferencing licenses assigned.

The next step is to verify the user's enterprise voice, onpreLineURI, voicemail, and so on. Here is the list of attributes and their expected status: `EnterpriseVoiceEnabled = $true, HostedVoicemail = $true`. You can change that status using the command `Set-CsUser bilag@bloguc.com -HostedVoicemail $true`

```
Get-CsOnlineUser -Identity bilag@bloguc.com | Select  
Display*,*upgrade*,*voice*, *LineUri* | fl
```

Additionally, you need to assign a voice routing policy and dial plan to the user. As an admin, you can check your existing Skype for Business On-Premises voice policy and replicate a similar PSTN route and usages with the online PSTN gateway, which you set up as part of Teams Direct Routing configuration (refer to Chapter 4).

Grant the user a previously created online voice routing policy (`Grant-CsOnlineVoiceRoutingPolicy`) using PowerShell and then verify the policy assignment using the PowerShell command `Get-CsOnlineUser`.

You can do staging work, including the voice routing policy, tenant dial plan, online PSTN gateway (with FQDN), calling policy, location based routing (LBR) and Teams emergency routing policy, ahead of user migration. This work will not disturb the users' existing call flow or any other features.

Redirect the DID from the existing SBC through Teams Direct Routing. For example, configure the SBC to route incoming DID calls to the Direct Routing trunk(s) instead of

the Skype for Business Mediation Server and then configure the SBC to route outbound calls to the PSTN provider (SIP trunk or PRI line) accordingly. This is the first step that is disruptive to the user and will start the outage window. Before making call routing changes from Skype for Business mediation pool to Microsoft Teams DR in SBC, all the users for the particular must be migrated to Teams Only mode.

The final step is to upgrade the user to Microsoft Teams. You can perform a single step move with Server 2019 or Server 2015 CU8+ using the command to move the user to Teams only mode.

```
Import-Module SkypeOnlineConnector
$Creds = Get-Credential
$SfbSession = New-CsOnlineSession -OverrideAdminDomain "<YourDomainName>.onmicrosoft.com" -Credential $Creds
Import-PSSession $SfbSession
$url = https://admin<1a>.online.lync.com/HostedMigration/hostedmigrationService.svc
Move-CsUser -Identity bilag@bloguc.com -Target sipfed.online.lync.com -MoveToTeams -Credential $creds -HostedMigrationOverrideUrl $url
```

Notice that before upgrading the user, and after the upgrade completes, the TeamsUpgradeEffectiveMode shows as TeamsOnly and TeamsUpgradePolicy is UpgradeToTeams, along with other attributes such as enterprise voice, OnPremLineURI, and so on. Figure 6-6 shows all attributes set up correctly after the user has been migrated to Teams only mode. And then assign voice routing policy and tenant dial plan as per the requirement.



Figure 6-6. User migrated to Teams only mode

As part of validation, you can capture the Teams client logs by pressing Ctrl+Alt+Shift+1 on the keyboard while keeping the Teams Windows desktop client on.

As an admin, you must think about how enabling these feature functions affects the users, as they might not be familiar with all the features of Teams. You have to design a user readiness strategy. First, define the value of Teams features for your end users; to do so, understand relevant personas, use cases, and usage scenarios. Remember that business goals (increasing productivity, saving money) are not always user goals [64].

Is it relevant to measure users' tendency to change? How much change is happening? What is your organizational change culture? Identify the relevant readiness channels, including awareness, training, and support. The most important advice is to communicate early. Don't wait for the completion of the technical readiness stage.

To build and implement your readiness plan, use the following procedure to inform your plan. Make sure to align this with your technical team and project lead.

1. Run the pilot. This allows validation of both technical and user readiness. It also allows the migration to be a formal effort with a defined test plan and clear go/no-go goals. It should also include a good representation of your user base.
2. Plan for coexistence, running Skype for Business and Teams together in your environment using several upgrade approaches (modes) to meet your organization's needs.
3. Finally, perform the upgrade by moving users to Teams only mode. You can plan for a phased approach that enables you to pause or mitigate if needed. Maintain momentum once you begin to avoid having users in too many modes.

After deployment, create an operational plan. As part of this plan, measure against your defined goals and mitigate as needed. Monitor network health to ensure a positive user experience.

For bulk user migration, you can create your own PowerShell script and then migrate multiple users at once. Here is a simple PowerShell script to migrate users from Skype for Business On-Premises to Teams. The input file is in .csv format with user UPN, voice routing policy, emergency routing policy, and dial plan.

```
#Script starts
function Select-FileDialog
{
```


CHAPTER 6 MIGRATION FROM SKYPE FOR BUSINESS (LYNC) ON-PREMISES AND ONLINE TO
MICROSOFT TEAMS

```
param([string]$Title,[string]$Directory,[string]$Filter="CSV Files
(*.csv)|*.csv")
[System.Reflection.Assembly]::LoadWithPartialName("System.Windows.
Forms") | Out-Null
$objForm = New-Object System.Windows.Forms.OpenFileDialog
$objForm.InitialDirectory = $Directory
$objForm.Filter = $Filter
$objForm.Title = $Title
$objForm.ShowHelp = $true

$Show = $objForm.ShowDialog()

If ($Show -eq "OK")
{
    Return $objForm.FileName
}
Else
{
    Exit
}
}

Start-Transcript -Path .\UserSfB-Teams_migrate.txt

$creds = Get-Credential
$sfboSession = New-CsOnlineSession -OverrideAdminDomain "<YourDomainname.
onmicrosoft.com" -Credential $creds
Import-PSSession $sfboSession -AllowClobber
$FileName = Select-FileDialog -Title "Import an CSV file" -Directory "c:\"
$csvFile = Import-Csv $FileName

foreach($entry in $csvFile){
    $user = $entry.sip
    $VoicePolicy = $entry.voicepolicy
    $Dialplan = $entry.dialplan
    $EmergencyPolicy = $entry.emergencypolicy
```

```
$url="https://admin<yourSfBOnline-Tenant>.online.lync.com/
HostedMigration/hostedmigrationService.svc"
Move-CsUser -Identity $user -Target sipfed.online.lync.com
-MoveToTeams -Credential $creds -HostedMigrationOverrideUrl $url
-Confirm:$False

#Assign Policy
Set-CsUser -Identity $user -EnterpriseVoiceEnabled $true
-HostedVoiceMail $true
Grant-CsOnlineVoiceRoutingPolicy -Identity $user -PolicyName
$VoicePolicy
Grant-CsTenantDialPlan -Identity $user -PolicyName $Dialplan
Grant-CsTeamsEmergencyCallRoutingPolicy -Identity $user -PolicyName
$EmergencyPolicy
}
Write-Host "Script Completed" -ForegroundColor Yellow
Stop-Transcript
#Script ended
```

Teams Only Experience for End Users

A Teams only experience means using Microsoft Teams for everything, including chat, audio and video calls, meetings, and content sharing. Here are the details of the experience a Teams only user has.

- *For chat and calling:* Teams only users will receive and initiate all chats and calls in Teams. They can do interoperable IMs or call with any Skype for Business users; also, they will be redirected to Teams if they try to sign in to Skype for Business clients.
- *For meetings:* Users will schedule all new meetings in Teams only. Teams Outlook meeting add-ins are enabled, and the Skype for Business add-in is disabled automatically.
- *For Teams only users:* All data are migrated to Teams, including existing contacts and buddy lists from Skype for Business, including federated contacts, but not distribution lists. Existing Skype for Business meetings (both On-Premises and Online) are converted to Teams meetings.

What Happens to Skype for Business During the Upgrade?

Skype for Business clients get a redirected experience, as shown in Figure 6-7. Skype for Business will go into meeting-only client configuration mode. This gives explicit notification to the user regarding guidance; it provides a secure link to Teams and also enables access to Skype for Business clients.

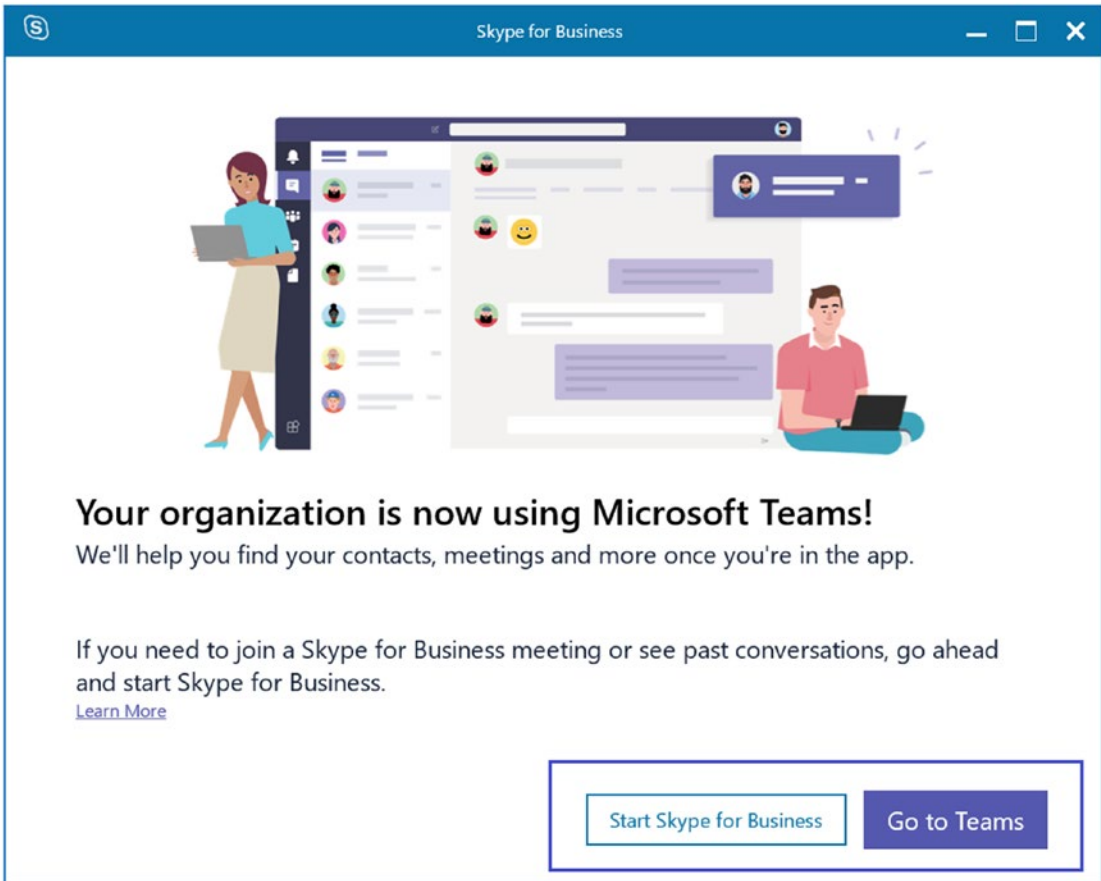


Figure 6-7. *Skype for Business experience after upgrade*

This Skype for Business client is focused primarily on meetings, and it does show meetings, as well as past conversation tabs. However, you cannot initiate chat and calls, and they are disabled. Figure 6-8 shows a meeting calendar to join meetings; however, the chat and call options are gone.

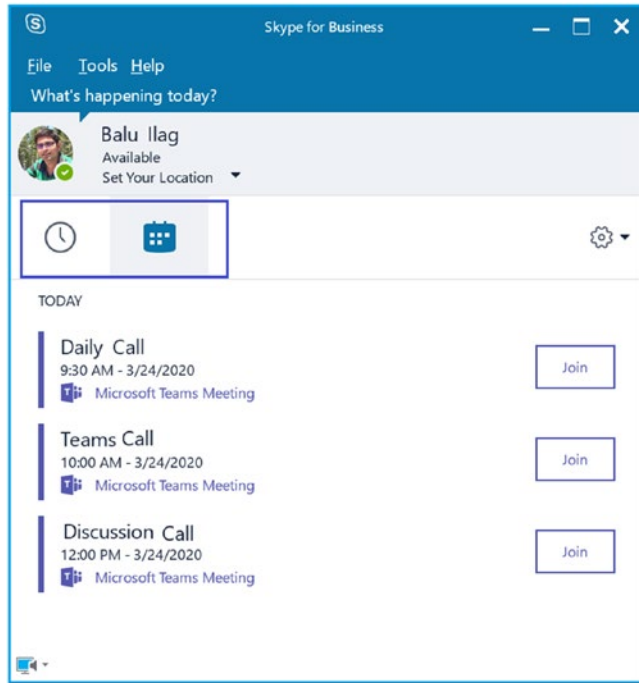


Figure 6-8. *Skype for Business experience after upgrade*

Regarding meetings, all the previous Skype for Business meetings are migrated to Teams. Users can still attend new Skype for Business meetings scheduled by others; however, they cannot schedule new Skype meetings, and Skype meeting add-ons will automatically be disabled. Therefore, users cannot see the Skype meeting schedule option in an Outlook calendar.

Because all the new meetings schedule in Teams and Skype for Business (received) are shown, when clicking on a Teams meeting in Skype for Business, it redirects to the Teams client. Similarly, selecting a Skype for Business meeting in the Teams app redirects to Skype for Business client.

Client Experiences Between Skype for Business and Teams

When you have a large organization with enterprise voice deployments, and you are choosing a group or site-wise user migration approach, you could have some users on

Skype for Business and the rest on Teams. Specific to the federation aspect, when your organization has moved to Teams but your partner organization is still on Skype for Business, what will the experience be like?

Native Interoperability Experience for One-to-One Chat and Call

When a Skype for Business user sends a chat message to a Teams only user, the result is shown in Figure 6-9. When a Teams user receives a chat message from a Skype for Business user, then he or she will see an indication that the person is currently using Skype for Business, and some Teams features won't be available. The user will not have the ability to use Giphys, emojis, or formatting options.

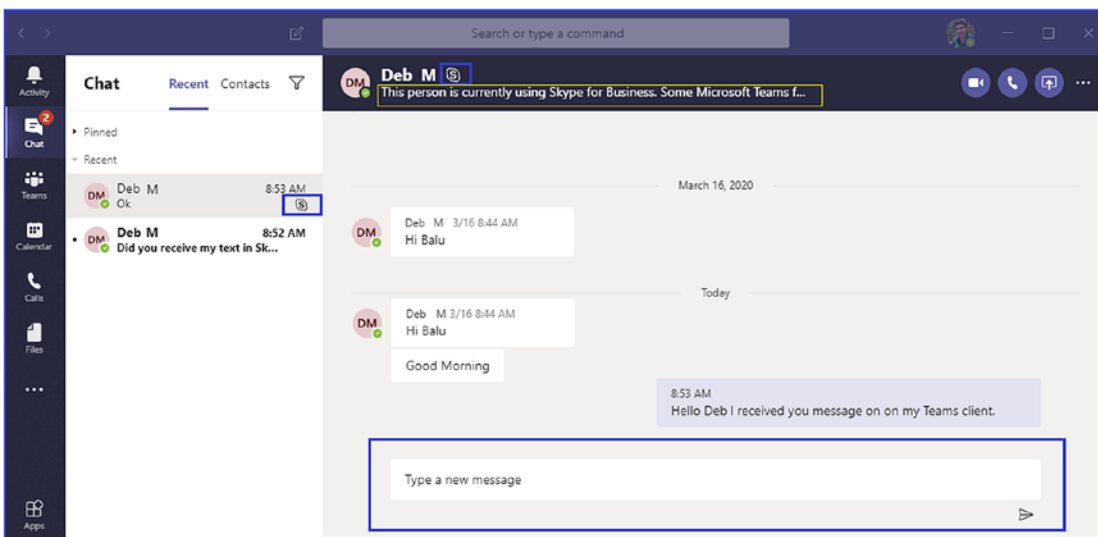


Figure 6-9. Interoperability message on Teams

On the Skype side, the experience is similar. A warning text message indicates that the person at the other end is not using Skype for Business, as shown in Figure 6-10.

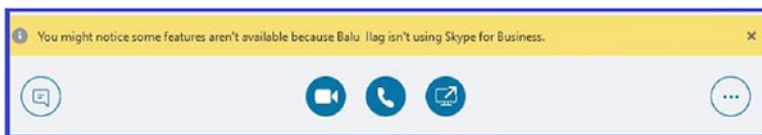


Figure 6-10. Interoperability message on Skype for Business

When the users call, the response is similar, including a warning message that using some Teams features won't be available when using Skype for Business. However, to see the notification a user must have the latest Skype for Business version of MSI and Click to Run version.

Native Interoperability Experience for One-to-One Desktop Sharing Between Teams and Skype for Business Client

When Skype for Business users communicate with Teams users, establishing an interoperability thread communicating via chat, audio, or video, the Skype for Business users are notified the recipient is not using Skype for Business in a yellow banner.

For desktop sharing, when Skype for Business users invoke desktop sharing, usually by clicking on a share desktop icon, they are presented with this notification message: "Click to start meeting to share the screen with Teams users." In this example, Skype for Business users talking to Teams users decide to share the desktop; the Skype client shows a notification the meeting will include desktop sharing (see Figure 6-11). The meeting link is shared across the Teams client so that Teams users can join the meeting; however, this is a Skype meeting, so the Skype client will launch, and both users have joined a Skype meeting. If Teams doesn't have a Skype client, then the user can join using a Skype Meeting app in the browser; however, this requires a one-time download.

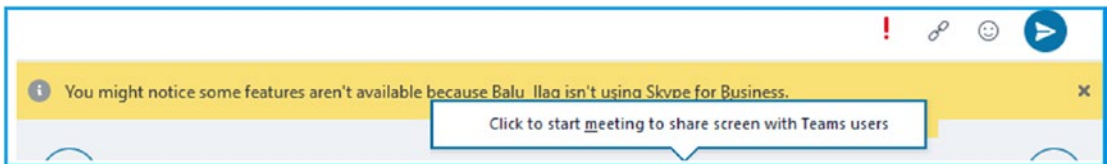


Figure 6-11. Interoperability experience for desktop sharing on Skype for Business

The peer-to-peer call desktop is not working for the user to start a meeting. Teams handles that back-end meeting setup on behalf of the user as an automated workflow and invites another participant to the meeting using desktop sharing.

The same things will work when Teams users start a desktop sharing with Skype for Business users. In this case, the Teams user initiating desktop sharing means the meeting URL is shared in Teams across Skype for Business. Skype for Business users can join with the client if the Teams client is not installed, as shown in Figure 6-12.

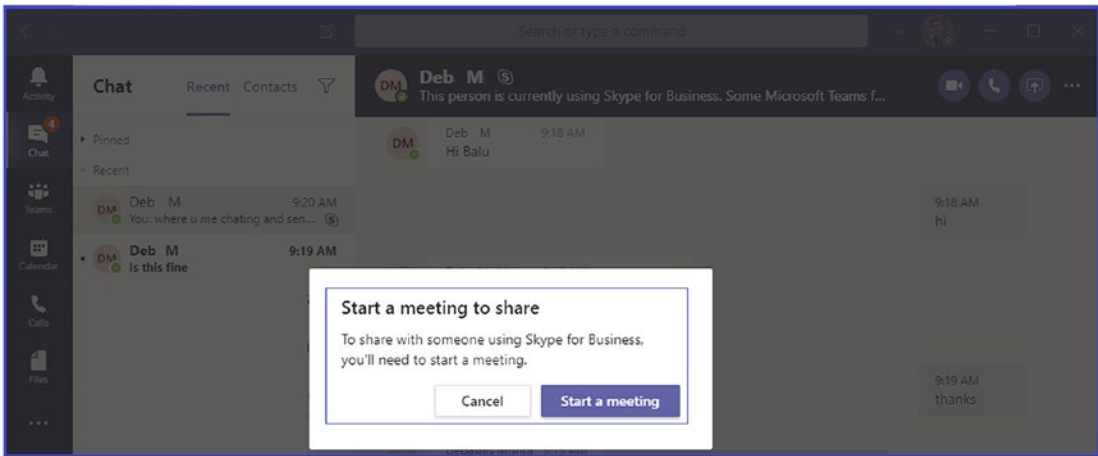


Figure 6-12. Interoperability experience for desktop sharing on Teams

Interoperability Meeting Joins Experience

Joining a Skype for Business meeting from Outlook or a Teams client will launch the Skype for Business client or meeting app if it is installed. If not, then joining via web requires a download.

Skype for Business meetings are joined via Skype for Business client only whether it is a Skype for Business full client or just the Meeting app. Similarly, Teams meetings always join via the Teams client, whether Teams desktop, mobile, or web app only. No cross-platform joining is allowed.

Migration Tips and Tools

In this section, you will learn about the available tools that assist in your Skype for Business to Teams migration efforts and help you troubleshoot meeting migration status.

Teams Meeting Migration Service Tool

Meeting Migration Service (MMS) is a back-end service that triggers when the Move-CsUser command runs using the Skype for Business Online PowerShell module. As an admin, you can check the status of running migrations, manually trigger meeting migrations, and disable migrations altogether. To check the status of meeting migrations,

you can use the `Get-CsMeetingMigrationStatus` command. For example, to get a summary status of all MMS migrations, run the following cmdlet, which provides a tabular view of all migration states.

```
Get-CsMeetingMigrationStatus -SummaryOnly
```

Figure 6-13 shows the meeting migration result.

```
PS C:\WINDOWS\system32> Get-CsMeetingMigrationStatus -SummaryOnly
MigrationType : All
State         UserCount
-----
Pending       3
InProgress    0
Failed        2
Succeeded     301
```

Figure 6-13. Meeting migration status

If you would like to check the status of migration for a user, you can use the `Get-CsMeetingMigrationStatus` command with the `Identity` parameter. For example, to check the status of migration for user `bilag@bloguc.com`, use this command.

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

As part of meeting management, you do enable and disable MMS, but MMS is enabled by default for all organizations. It can also be disabled on different levels, though; for example, it can be disabled entirely for the tenant and disabled only for changes related to Audio Conferencing (where MMS will still run when a user is migrated from on-premises to the cloud or when granted `TeamsOnly` mode or `SfbWithTeamsCollabAndMeetings` mode in `TeamsUpgradePolicy`). To check if MMS is enabled for your organization, run the following [64] command.

```
Get-CsTenantMigrationConfiguration
```

MMS is enabled if the `MeetingMigrationEnabled` parameter is `$true`.

Tips for User Migration

1. Make sure to assign and enable all required licenses, such as Teams license, Skype for Business Plan2, Phone System, and Audio Conferencing, for all users who are being migrated.
2. Assign and enable licenses at least 24 hours before user migration, so that licenses will be enabled and applied properly.
3. By default, the PowerShell module connection to Skype for Business Online times out after an hour. Use `Enable-CsOnlineSessionForReconnection` after importing a PowerShell session for Skype for Business Online so when you are doing bulk user migrations, the PowerShell connection reconnects automatically.
4. After migration, user attribute and policy reflection takes a long time. Plan user migration on a Friday so that when users come back on Monday their accounts will be ready with full functionality, including voice routing policy, dial pad, contact lists, recurring meetings, and so on.

Skype for Business to Teams User Migration Tool

The Skype for Business On-Premises/Online to Microsoft Teams migration tool (version 1) is available for download at <https://bloguc.com/download/17154/>. This tool does have the following prerequisites.

1. The on-premises user account must be synced with Azure AD and available in the Office 365 admin portal.
2. The user account must have Microsoft Teams and Skype for Business Online (plan2) licenses assigned.
3. If migrating a user account enabled for enterprise voice (On-Premises/Online), then assign Audio Conferencing and Phone System licenses to the user account before migrating.
4. To migrate Skype for Business On-Premises to Teams, run this tool on the Skype for Business front-end server.

5. To migrate Skype for Business Online to Teams only mode, run this tool on Windows 10 or Windows Server 2012/2016 with the latest PowerShell module and skypeonlineconnector module.
6. The account you are using to run this tool must have Skype for Business On-Premises server (CsAdministrator or CsServerAdministrator) as well as Office 365 global admin or user admin role permissions.

Here are the assumptions made for the process.

- Skype for Business Server 2015 environment has CU8 applied (minimum).
- The user is enabled for enterprise voice using on-premises PSTN.
- The user who is getting migrated must have Microsoft Teams, Skype for Business Online (Plan2), Phone System, and Audio Conferencing licenses assigned (Phone System and Audio Conferencing licenses require an enterprise voice-enabled user to migrate to Teams for enterprise voice support).
- Tools are applicable to Skype for Business Server 2015, Skype for Business Server 2019, and Skype for Business Online.

Once you download the tool (<https://bloguc.com/tools/>), the next thing you need to do is to copy this tool to the Skype for Business front-end server, or your Windows machine based on the migration scenario.

Scenario 1: Skype for Business On-Premises to Teams Only Mode with Enterprise Voice-Enabled User

1. Copy the SFB to Teams migration tool v1.0 or earlier to your Skype for Business front-end server.
2. Double-click the Skype for Business to Teams tool and run prerequisites to validate PowerShell and the SkypeOnlineConnector module. Figure 6-14 shows the prerequisites.

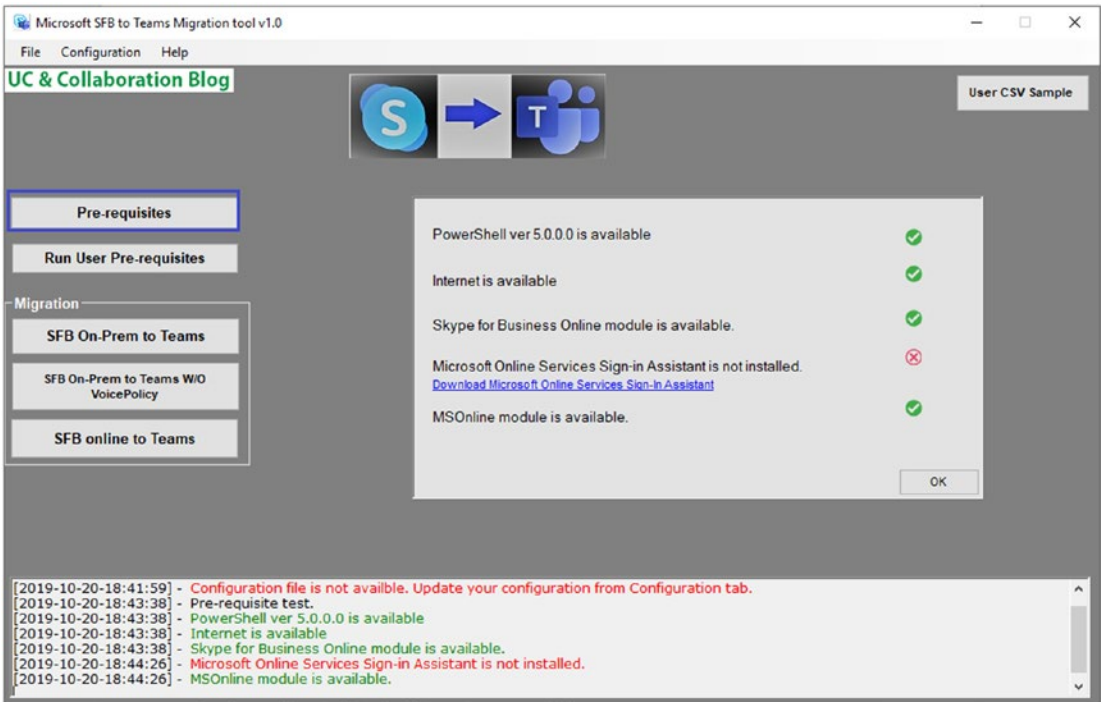


Figure 6-14. Checking the prerequisites

3. Update the configuration with your tenant name and Skype for Business online URL. Click Save and click Exit, as shown in Figure 6-15.

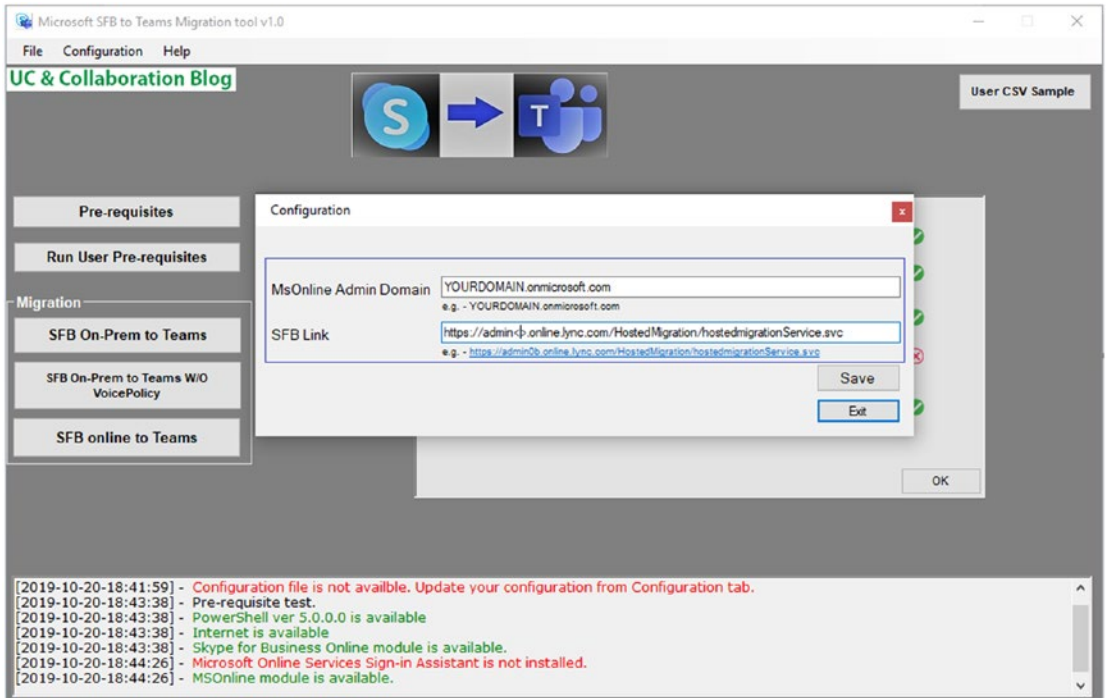


Figure 6-15. Update configuration

4. Download the User CSV sample format input file and update the user SIP address, voice routing policy, dial plan, and emergency policy for all users who are being migrated to Teams (SIP address is mandatory to input).
5. Click SFB On-Prem to Teams and select the input user CSV file that you updated in Step 4.
6. Enter the Office 365 admin credentials, as shown in Figure 6-16, and click OK. The tools will take care of everything else. The tool will migrate all users to Teams and write migration status reports (check prerequisites for permission).

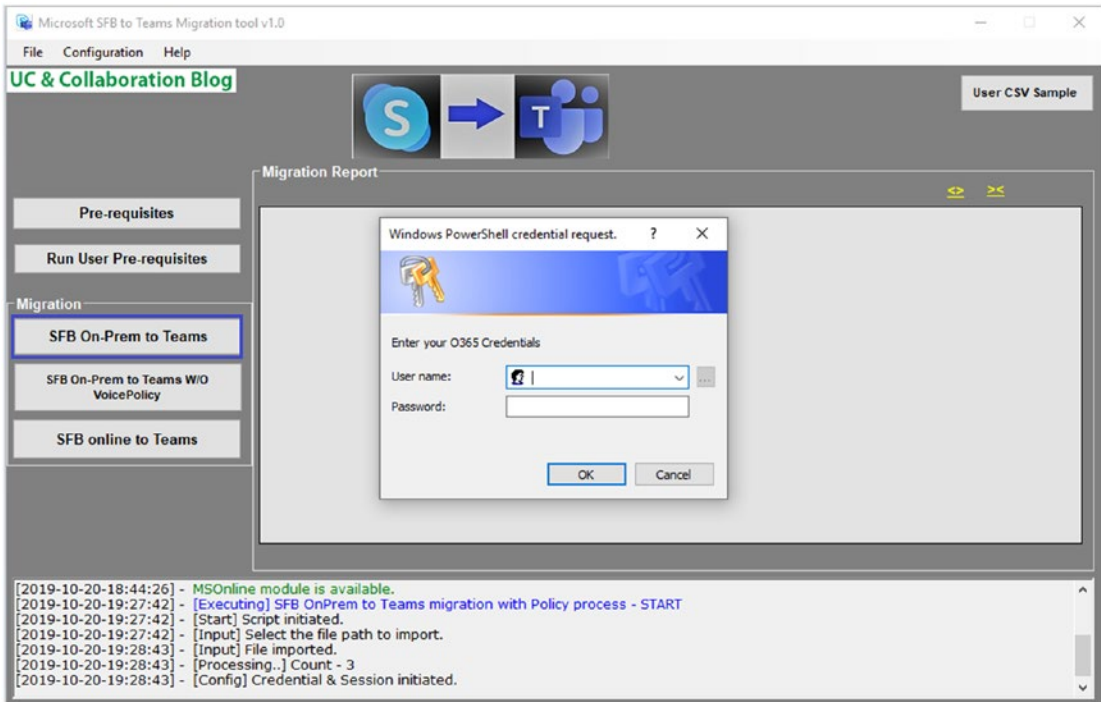


Figure 6-16. Entering Office 365 credentials

Scenario 2: Skype for Business Online to Teams Only Mode

This scenario is technically granting Teams upgrade policy, so does not involve much user migration.

1. Double-click the SFB to Teams migration tool v1.0 and check prerequisites and update.
2. Click the Configuration tab to update your tenant and Skype for Business online URL.
3. Download and update the user CSV input file.
4. Click SFB Online To Teams and select User Input File. Enter Office 365 admin credentials and let the tool take care of everything else.

Summary

In summary, as an admin, you must build and implement a readiness plan, using the following three-step process that includes overall migration. In the overall migration, a critical facet is user readiness and enterprise voice implementation. As part of prep work, you can do staging work including the voice routing policy, dial plan, and online PSTN gateway (with FQDN) ahead of user migration. This work will not disturb the users' existing call flow or any other features. Align with your technical team and project lead.

Here is the three-step process.

1. Run the pilot. This allows validation of both technical and user readiness. It also allows this to be a formal effort with a defined test plan and clear go/no-go goals. Make sure to include a good representation of your user base.
2. Plan for coexistence, running Skype for Business and Teams together in your environment using several upgrade approaches (modes) to meet your organization's needs.
3. Finally, perform the upgrade by moving users to Teams only mode. You can plan for a phased approach that enables you to pause or mitigate if needed. Maintain momentum once you begin to avoid having users in too many modes.

After the deployment, create an operational plan. As part of that plan, measure against your defined goals and mitigate as needed. Make sure to monitor network health to ensure a positive user experience. Maintain user excitement to sustain adoption and return on investment. Plan for product innovations to optimize and grow.

CHAPTER 7

Microsoft Teams Troubleshooting Approaches

In this chapter, you will learn different functionalities of the Teams app, including call quality and meeting troubleshooting. Also, you will learn about basic scenarios including Teams sign-in issues, policy-related issues, tenant configuration, network configuration, and management with a simple approach.

Because Microsoft Teams is a cloud-only application, that puts some limitations on administrator-based troubleshooting. Unlike Office Communication, Lync, or Skype for Business, where you as an admin were doing end-to-end troubleshooting, in Microsoft Teams back-end server and services are managed by Microsoft; therefore you will be doing mainly client-side troubleshooting based on information provided by Microsoft. This chapter covers three aspect of Teams troubleshooting: user login issues, call quality (one-to-one calls and meetings) issues, and PSTN call issues. Additionally, you will learn tools that can help you in troubleshooting.

Microsoft Teams Foundation Details That Help in Troubleshooting

Teams provides chat, audio and video calls, meetings, content sharing, and application integration. These features all coming from dependent services in Teams. For example, voicemail messages within Teams require an Exchange Online mailbox. The connection point is from the Teams client to the mailbox, and playing voice messages in the client

requires a player. Next-generation Calling PSTN is used for Teams PSTN using a Calling Plan and Phone System license. You cannot provision users without a Teams license. If anyone turns off the Skype for Business Online license, then that user is deprovisioned, so do not turn off Skype for Business Online, which is required for Teams.

The Teams business voice directory is where Microsoft stores user attributes. With respect to calling, reverse number lookup (RNL) happens against the business voice directory attributes.

If you have a phone number assigned and it appears in Skype for Business Online, but users get a 404 not found error for the inbound call, that is because Teams is not looking user attributes in Skype for Business Online. The phone number attribute is in a different directory, and it replicates with Skype Online, and so on. Therefore, if one feature is not in Teams, you might need to check the dependent service for that feature. As an admin, you need to allow Teams services, IP addresses, ports and protocols, URLs, and FQDNs for each feature to work correctly. As part of troubleshooting, you should identify and use the core tools for Microsoft Teams deployment, collect diagnostic information from Teams clients, troubleshoot common Teams problems, and so on.

Teams Features and URL Dependency

The following is a list of URL dependencies.

- Teams authentication is dependent on `Teams.microsoft.com` and `login.microsoft.com`.
- Teams chat and presence features are dependent on some URLs, so if chat or presence are not working correctly, then the first thing to check is that the following service URLs are accessible from the computer of the user who is facing an issue.
 - `amer.ng.msg.teams.microsoft.com` (one-to-one chat)
 - `chatsvcagg.teams.microsoft.com`
 - `presence.teams.microsoft.com`
 - `nortcentralus.notifications.teams.microsoft.com`
 - `statics.teams.microsoft.com`
 - `media.giphy.com`
 - `us-api.asm.skype.com`

- Calling and live events are dependent on `api.fliproxy.teams.microsoft.com`, `teams.registrar.prod.v2`, and `broadcast.skype.com` service URLs.
- Settings are dependent on `config.edge.skype.com`, `config.teams.microsoft.com`, and `teams.api.mt.amer.beta` service URLs.
- Office 365 and Skype for Business are dependent on the service URLs `bloguc-my.sharepoint.com`, `bloguc.sharepoint.com`, `outlook.office.com` for voicemail messages, `*.officeapps.live.com`, and `substrate.office.com`. (You can replace your organization name with Bloguc.)
- Telemetry functionality is dependent on service URLs like `pipe.skype.com`, `mobile.pipe.aria.microsoft.com`, and `Watson.telemetry.microsoft.com`.

Why Do I Care About Network Traces in Teams?

The Microsoft Teams app makes a direct connection to many services. That's why you, as admin, must know the https tracing and tools to identify what is blocking the Teams connections. It might be your firewall or proxy, which you can see in https traces by looking at the response coming back from the Teams service.

You can get traces in a web browser using a browser like Microsoft Edge or Google Chrome with an F12 function key. Selecting Dev tools, then reproduce the issue and save traces to HTTP Archive (HAR) files and open in Fiddler, Charles, or Notepad++ (you can find these tools by searching in Google). These are all third-party tools, but they help you in viewing https traces. Https tracing can be helpful for connectivity issues and for getting information about the client configuring and settings, as not everything is logged to Microsoft Teams diagnostics. Depending on the client platform, you might be able to use what already exists if the client has Edge or Chrome installed. Then just connect to `Teams.microsoft.com` via the browser with the development tools open. These tools can also be used to view some details about the Teams client behavior and even local storage.

Microsoft Teams Sign-in Issues

Microsoft Teams Administrative Roles

Microsoft Teams provides some administrative roles to allow full access to all of the Teams service settings, such as the Global admin and the Teams admin. Other roles only provide access to certain parts of Microsoft Teams to perform recurring tasks, such as troubleshooting call quality problems and managing telephony settings. As of this writing, Microsoft Teams doesn't support role-based access control (RBAC) to build a custom role. However, it does provide four built-in admin roles: Teams admin, Teams communication admin, Teams communication support engineer, and Teams communication support specialist. These admin roles are specific to Teams and do not grant permissions to other services, such as Exchange Online or SharePoint Online.

Microsoft Teams provides the ability to do more than just make simple PSTN phone calls, with dial plans, call routing, auto attendants, and more.

For overall Teams administration, Microsoft provides an admin tool called Microsoft Teams admin center, which allows admins to operate and create teams, to create Teams policies, manage phone devices and telephone numbers, manage locations and emergency addresses, and manage meeting settings and policies, such as live event settings and policies, messaging policies, the Teams apps settings and policies, organization-wide settings for sharing, guest access, resource accounts, and all calling settings. Refer to Chapter 2 for complete Teams admin center details. To access the Teams admin center, a user must be allocated to one of the following admin roles:

- Global administrator
- Teams service administrator
- Skype for Business administrator (this is a legacy role and might be removed in the future)
- Teams communications administrator
- Teams communications support engineer
- Teams communications support specialist

How Teams Authentication Works

Microsoft Teams out of the box supports modern authentication (MA). This authentication process permits users to sign-in to a Teams application securely. MA includes single sign-on (SSO), which helps users log in on the Teams app without entering credentials (the user has to enter credentials the first time). Basically, SSO is a process that allows Teams to know that users have already entered their credentials, such as work email addresses and passwords, elsewhere, and they should not be required to enter their credentials again to log in to the Teams app.

Because Microsoft Teams supports MA, the Teams app has been provided with MA hard-coded into it, and it should be able to recognize user credentials as linked to their Office 365 account. If a user is unable to log in to Teams, there might be something wrong with that user's Office 365 account, like an expired or incorrect password, no license assigned, and so on.

Teams Sign-in Issues and Corresponding Error Codes

If users receive an error code when logging in to Teams, you, as an admin, must take appropriate action. Table 7-1 shows a list of error codes and the actions that should be taken.

Table 7-1. *Teams Known Issues [98]*

Code	Description	Troubleshooting Action
0xCAA20003	You ran into an authorization problem.	Make sure your date and time are set up correctly. Whether your date and time are accurate will affect your ability to connect to secure sites (https).
0xCAA82EE2	The request has timed out.	Ensure that you are connected to the Internet. Then work with your IT admin to ensure that other apps or a firewall configuration aren't preventing access.
0xCAA82EE7	The server name could not be resolved.	Ensure that you are connected to the Internet. Then work with your IT admin to ensure that other apps or a firewall configuration aren't preventing access.

(continued)

Table 7-1. (continued)

Code	Description	Troubleshooting Action
0xCAA20004	Your request needs to be approved by a resource owner or authorization server.	Contact your IT admin so they can confirm that your organization is complying with Azure AD configuration policies.
0xCAA90018	You're not using the right credentials.	The Windows credentials you signed in with are different than your Office 365 credentials. Try to sign in again with the correct email and password combination. If you continue to receive this status code, contact your IT admin.
none	You'll need to re-enter your PIN using a smart card.	Reinsert your smart card. Also, your smart card certificate might be corrupt. In that is the case, contact your IT admin.

Microsoft Teams sign-in issues are generally broken into several categories.

- Generally, *authentication issues* happen when users might not be entering their sign-in address (email address) or password correctly, and the Teams back-end service might not authenticate the user. This happens for different reasons.
 - The credentials (email address and password) users entered are incorrect; generally, in Teams, we use User Principal Name (UPN) and password.
 - Teams authentication is also dependent on accurate time information on the user's computer, including the affected user's computer, which is configured to the wrong time zone, or maybe the computer clock is incorrectly set.
- *Teams account provisioning* issues occur if users are not be enabled for Teams, or they are enabled, but not authorized to sign in. That can check by checked by logging in to the Office 365 portal. Apart from provisioning, the user account might not be synced correctly to Office 365 (directory synchronization is not happening). To check if an account is enabled for Teams and authorized for sign-in, follow these steps.

- a. Log in to Office 365 portal (<https://admin.microsoft.com/AdminPortal/Home#/users>) and navigate to Users. Find the affected user and then open user properties.
- b. Validate that the Teams license is enabled, and check that the user allowed for login, as shown in Figure 7-1.

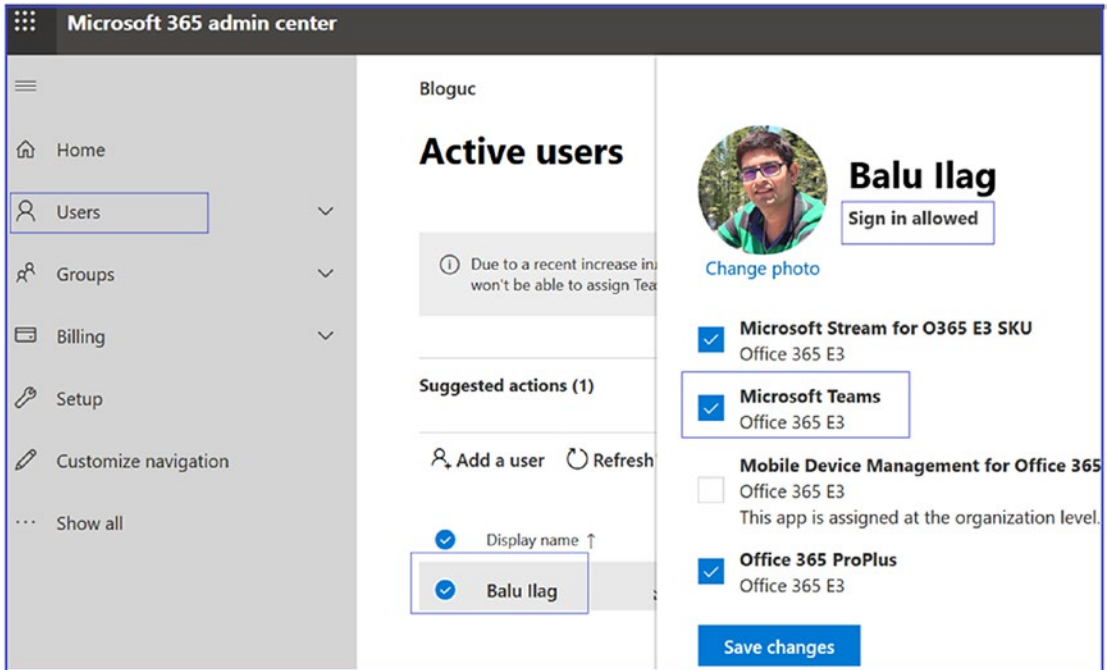


Figure 7-1. Checking account provisioning

- *The Microsoft Teams app itself* might have an issue. Perhaps the Teams app is not installed correctly on a user's computer, causing problems with reaching the Office 365 services. Maybe the network that the user has connected to has connectivity issues. To resolve the Teams app issue, you could first update Teams and then check that Internet is working correctly.
- The last category is *Teams back-end cloud service-related issues*. When there are service-related issues, all users in a tenant are affected or some users are affected at the back-end datacenter or region.

- You can collect the Teams diagnostic log and check if there are any issues. When reading these sign-in logs, pay attention to the first few errors or warning messages, as these will indicate the issue.

Approaching Teams Issues

Every admin has an individual approach to troubleshooting any issues. Here is the fundamental but beneficial approach that I take whenever dealing with any problem. For example, often admins receive complaints via call, incident report, or email that a user is unable to log in to the Microsoft Teams client. Here is the series of steps you can perform to solve the problem. The most important thing is the approach to the issue.

1. *Understand the problem:* What is not working? Is there any error message provided by the user? If there is not enough information, reach out to the user and make sure you understand the problem first. Once you grasp the problem, move on to Step 2.
2. *Check if there is any pattern:* Is more than one user facing the issue? Is the whole site down, or just a single user?
 - a. If more than one user is facing a log-in problem, then check if they are located in the same office, on the same network, and so on.
 - b. If a single user is affected, check if that user is enabled for Microsoft Teams license. Check if the Teams sign-in ever worked or this is the first time the user is trying to sign in.
 - i. Enabling a Teams license takes up to 12 hours. Typically a license is synced within an hour, but it sometimes takes longer.
 - ii. Check login credentials, as user passwords might have changed, been locked out, or expired.
3. *Check if the problem is with the Teams app:* Try different Teams apps.
 - a. Try with the Teams desktop app (Windows and macOS).
 - b. Use a mobile app (iOS or Android).

- c. Try with Web browser sign-in using incognito mode (kind of isolated mode).
 - d. If a specific client shows the issue, then clear the client cache and check again.
4. *Check different computers and different networks:* If all Teams apps show an error, then check internal vs. external networks (using a mobile hotspot if no external network is available).
 5. *Check if Teams login URLs are accessible:* If not, check with your network team to allow Teams communication.
 6. If the issue still persists, then you can troubleshoot the issue with the information gathered, or you can open a support case with Microsoft.

Collecting Teams Client Logs

Microsoft Teams has three kinds of log files: debug logs, media logs, and desktop logs. Usually an admin can read debug logs to find the cause of Teams features not working; however, media and desktop logs are only needed if requested by Microsoft support when you open a support case with Microsoft.

Microsoft Teams makes log collection reasonably easy. Just press a series of keys, and the Teams debug log will be collected and stored in the Downloads folder. Teams have different apps for different platforms, and each Teams app has a different method to collect logs; in addition, their log files are stored in a different location. Here are the details for each Teams app with the process for collecting a log.

First, the Teams debug log is the most common log. It is used for debugging Teams functionality and app-related issues. When you open a case with Microsoft support, they might ask you to generate a debug log. To read this log, you can use any text-based editor.

To generate a debug log for a Teams Windows client, follow this procedure.

1. Log in to the Teams client and then attempt to reproduce the issue, whether it is a call, chat, meeting join, desktop sharing, and so on.
2. While keeping the Teams Windows desktop client open, press **Ctrl+Alt+Shift+1** on your keyboard. The Teams debug log is automatically downloaded and saved to the %userprofile%\Downloads folder, as shown in Figure 7-2.

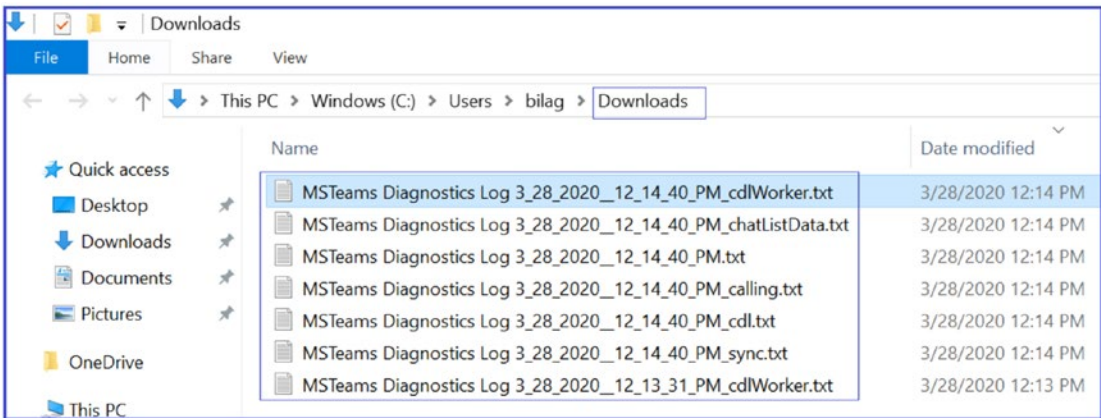


Figure 7-2. Downloaded Teams debug log

For a Teams macOS client, follow these steps.

1. Log in to the Teams macOS client and then attempt to reproduce the issue, whether it is a call, chat, meeting join, desktop sharing, and so on.
2. While keeping the Teams desktop client open, press Option+Command+Shift+1 on your keyboard. The Teams debug log will be stored under downloads.

Note For the web browser, the Teams web app will prompt you to save the debug logs.

The Teams media log includes information about audio and video calling and desktop sharing. This log is needed when you open a Microsoft support case, as it will be inspected by Microsoft support personnel. You don't have to do anything special to generate this log. It is automatically stored in the following paths.

- You can find the Teams Windows client media log at the following locations.
 - %appdata%\Microsoft\Teams\media-stack*.blog
 - %appdata%\Microsoft\Teams\skylib*.blog
 - %appdata%\Microsoft\Teams\media-stack*.etl

- You can find the Teams macOS client media log at the following locations.
 - `~/Library/Application Support/Microsoft/Teams/media-stack/*.blog`
 - `~/Library/Application Support/Microsoft/Teams/skylib/*.blog`

The Teams desktop client log is identified as a bootstrapper log. It includes log data that occur between the desktop client and the browser. Similar to the media log, this log also is needed primarily when it is requested by Microsoft support personnel. This log can be viewed via text editors.

To get the desktop log on a Teams Windows client, right-click the Microsoft Teams icon in your application tray, and select Get Logs as shown in Figure 7-3.

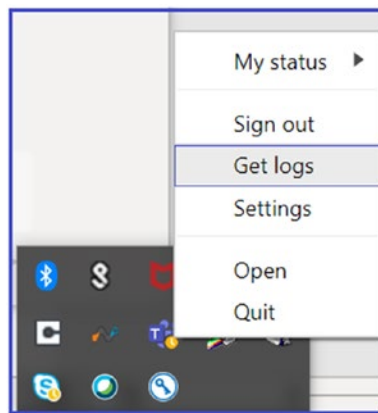


Figure 7-3. Getting the Teams desktop log

Teams desktop logs are stored on the path `%appdata%\Microsoft\Teams\logs.txt`.

For the Teams macOS client, from the Help pull-down menu, select Get Logs. Logs are then automatically saved to the path `~/Library/Application Support/Microsoft/Teams/logs.txt`.

Microsoft Teams Client-Side Troubleshooting

This topic covers Microsoft Teams client software installation and connectivity problems. To provide a consistent and positive experience to Teams end users, the client must be properly working without any issues. In this section, you will learn about troubleshooting Teams client installation and update issues, as well as Teams client connectivity issues.

Teams Client-Side Troubleshooting

Microsoft has provided Teams client apps for desktop (Windows and macOS), mobile (iOS and Android), Linux clients, and Web clients. Users get similar experiences using these clients.

The Teams client is part of the Office 365 suite, so when the user installs Office 365 Pro-plus as Click to Run, the Teams client is automatically installed. Admins can perform a managed microsoft installer (MSI) install as well.

If the Teams client is having issues like not starting, restarting, hanging, and so on, then follow these steps to resolve client-side issues.

1. When Teams client shows the issue, the first thing to do is update the Teams client. Teams client auto-updates, but it is best practice to check for client updates. To do so, select your profile picture, and then select Check For Updates, as shown in Figure 7-4, to install any available updates.

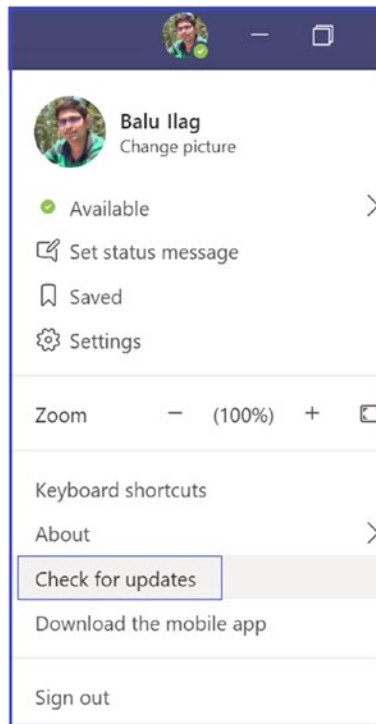


Figure 7-4. *Checking for Teams client updates (desktop client)*

2. If the issue persists after the Teams client updates, the next thing to do is check the client installer log. When the Teams client is installed, the Teams installer logs track the sequence of events. The installer log can be found at %LocalAppData%\SquirrelTemp\SquirrelSetup.log. Check this log to see if there is any error message or a call stack near the end of the log. Note that call stacks at the beginning of the log might not mean that an installation issue exists. It can be easier to compare the affected computer log against the log from a successful installation (even on another computer) to see what is expected.
3. If an issue persists, then uninstall the Teams client entirely and then log in to the Teams web client using <https://teams.microsoft.com>. Perform a desktop install by clicking on the profile picture and then downloading and installing the Teams desktop app.

Microsoft Teams has various limitations and expiration periods applied for each feature: persistent chat, voice and video calls, meeting, application sharing, file sharing, and so on. In Microsoft Teams, every workload has a different maximum limit set by Teams (back-end) services. Here I elaborate on maximum limits and expirations for Teams meetings, chat, live events, PowerPoint file uploads in a meeting, file store, and so on.

As an admin, you must know when and how Teams expiration and the maximum limit applies. This information will save troubleshooting time, so carefully review these limits and specifications.

What Are the Teams Meeting Expiration Limits?

Microsoft Teams does provide different meeting scenarios, and every meeting scenario has a different expiration period defined. For example, a Teams regular meeting conference ID expires after start time plus 60 days. After the meeting expiration, if a user tries to join a Teams meeting by dialing in to the conference ID, he or she will hear a message indicating that the conference ID entered is not valid [104].

1. *Teams Meet Now*: This type of meeting expires after the start time plus 8 hours; this meeting scenario does not extend the expiration period, as this is an ad-hoc meeting.
2. *Regular meeting with no end time*: This type of meeting expires after the start time plus 60 days, and this meeting scenario extends the expiration period each time a user starts or updates a meeting, up to 60 days.
3. *Regular meeting with end time*: This type of meeting expires after the meeting end time plus 60 days. This meeting scenario extends the expiration period each time a user starts or updates a meeting, up to 60 days.
4. *Recurring with no end time*: This type of meeting expires after the start time plus 60 days. This meeting scenario extends the expiration period each time when a user starts or updates a meeting, up to 60 days.
5. *Recurring with end time*: This type of meeting expires after the end time of the last occurrence plus 60 days. This meeting scenario extends the expiration period each time a user starts or updates a meeting, up to 60 days.

What Is the Maximum Number of Participants Who Can Join a Teams Meeting?

In any Teams meeting at any given time, the number of people in a meeting is 250 (Microsoft increased number of participant limit as 300), irrespective of whether they dial in join or through a Teams app (Windows, macOS, mobile, or web).

For larger meeting scenarios, including organization-wide meetings, use the Teams live event feature, which is scalable up to 10,000 attendees with limited interaction like Q&A, Yammer post etc. Teams live event concurrent event limit is 50 event across tenant.

Note There is no limit set on how many Teams meeting can be hosted in one Office 365 tenant.

What Is the Maximum PowerPoint Presentation File Size Allowed in a Team Meeting?

Teams allows sharing content in Teams meetings and peer-to-peer calls. You can share and present PowerPoint presentations in a Teams meeting, for example. However, there is a specific file size limit allowed, up to 2 GB. You cannot share or upload files larger than 2 GB in Teams meetings.

What Is the Maximum Audience Limit of Teams Live Events?

Microsoft Teams live events are used for large broadcast meetings, such as all-staff meetings. The live event audience size maximum limit is 10,000 attendees and the maximum duration is 4 hours. A user can host concurrent live events in an Office 365 tenant. However, as of this writing, you can host a maximum of 15 concurrent Teams live events in your organization.

What Is the Maximum Limit in Teams and Channels?

Microsoft Teams does have a maximum limit specified for Teams and channels features. Here is the list of features with their limits.

- The number of teams a user can create is the maximum of 250 objects, meaning a user can create a maximum of 250 teams. Remember, for the 250-object limit, any directory object in Azure AD counts toward this limit. Global admins are exempted from this limit.

- The maximum number of teams a user can be a member of is 1,000. Individual users therefore cannot be part of more than 1,000 teams.
- The maximum number of members in a team is 10,000. The previous limit was 5,000 members, but Microsoft has increased this limit.
- The maximum number of owners per team is 100. It is best practice to have more than two owners of a team to handle a single-point failure situation.
- The number of organization-wide teams allowed in any Teams tenant organization is five, so use the organization-wide teams wisely.
- The maximum number of members in an organization-wide team is 10,000, so you cannot have more than 10,000 members in one organization-wide team (the previous limit was 5,000 members).
- The number of teams a global admin can create is 500,000.
- The number of teams an Office 365 tenant can have is 500,000. This limit includes archived teams.
- The number of channels per team is limited to 200, and this includes deleted channels.
- Another significant limitation in Teams is that each team can have a maximum of 30 private channels, so use private channels carefully and create them only when it is required.

Note In Teams, deleted channels can be restored within 30 days. During these 30 days, a deleted channel continues to be counted toward the 200 channel per team limit. After 30 days, a deleted channel and its content are permanently deleted, and the channel no longer counts toward the limit.

Microsoft Teams Chat Limitations

In Teams, users who participate in chat conversations must have an Exchange Online (cloud-based) mailbox for an admin to search chat conversations. That's because conversations that are part of the chat list are stored in the cloud-based mailboxes of the chat participants. If a chat participant doesn't have an Exchange Online mailbox,

the admin won't be able to search or place a hold on chat conversations. For example, in an Exchange hybrid deployment, users with on-premises mailboxes might be able to participate in conversations that are part of the chat list in Teams. However, in this case, content from these conversations is not searchable and cannot be placed on hold because the users don't have cloud-based mailboxes. So, keep this limitation in mind when you are using an Exchange hybrid environment.

Teams chat works on an Exchange back end, so Exchange messaging limits apply to the chat function within Teams as well. The maximum number of people in a private chat is 250.

If you have more than 20 people in a chat conversation, then the chat features such as Outlook automatic replies, Teams status messages, typing indicator, video and audio calling, sharing, and read receipts are turned off.

Another limitation is for files. The maximum number of file attachments in a chat conversation is 10. If the number of attachments exceeds this limit, then the chat participants will see an error message.

Teams Emailing a Channel Limitation

Sending an email to a team is a frequently used feature. If users want to send an email to a channel in Teams, they use the channel email address. When an email is part of a channel, anyone can reply to it to start a conversation. Here are some of the applicable limits for sending email to a channel.

- The message size limitation is 24 KB. If the message exceeds this limit, a preview message is generated, and the user is asked to download and view the original email from the link provided.
- The next limitation is for attachments. The number of file attachments is limited to 20. If the number of attachments or images exceeds this limit, the user will see an error message.
- The attachment size of each file is up to 10 MB. You cannot attach a file larger than 10 MB while sending to Teams.
- The limitation for the number of inline images is 50.

Note Message size, file attachment, and inline image limits are the same across all Office 365 licenses.

What Is the Limitation for Teams Channel Names?

Microsoft Teams channel names cannot contain characters or words such as ~ # % & * { } + / \ : < > ? | ' " and characters in ranges 0 to 1F and 80 to 9F.

Additionally, the words that are not allowed include, forms, CON, CONIN\$, CONOUT\$, PRN, AUX, NUL, COM1 to COM9, LPT1 to LPT9, desktop.ini, and _vti_. Also, Teams channel names cannot start with an underscore (_) or period (.), or end with a period (.).

Teams Client Connectivity Troubleshooting

A majority of Teams connectivity issues are due to the corporate firewall or proxy blocking Teams service URLs, FQDNs, IP addresses, or ports. It is worth verifying that the required URLs, FQDNs, and IP addresses are allowed through a corporate firewall or proxy. To get a list of Teams URLs, FQDN, IP addresses, and ports, visit the Microsoft document at <https://support.office.com/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2>.

Teams Audio and Video Call Quality Issue Troubleshooting

Microsoft Teams provides real-time audio and video calls and meetings (VoIP) and many other features. When users start using Teams for making audio and video calls and organizing meetings, they might feel a caller's audio breaking up or chopping in and out of a call or meeting. When someone shares video, it might freeze, pixelate, or disconnect. All these issues are due to the IP packets that represent audio and video traffic facing network loss, encountering congestion, and arriving out of sequence. This results in a poor user experience, and eventually users will hesitate to use Teams. To overcome these network issues, you should tackle these problems when you see the issue, or even before seeing the issue, if you implement QoS.

The majority of Teams call quality issues are related to a poor network, but sometimes they are due to resource constraints on the endpoint or the user's device. Particularly for the network, if you see high packet loss, latency, and jitter, then you need to work with your network admin to optimize the network. These issues are described here.

- Jitter explains the event where media arrives at different rates, which results in missing words or syllables in calls.
- Packet loss defines the occurrence where packets in a data transfer are dropped and missing. This will result in lower voice quality and speech that is hard to understand.
- Latency (delayed round-trip time [RTT]) means that media packets require a longer time to reach their destinations. Users will experience noticeable delays between two parties in a conversation, for example, causing people to speak at the same time.

Improving Teams call quality by solving these network quality issues boosts the overall available bandwidth for data connections, both internal and external to the network (Internet). Quality issues are caused by low bandwidth for certain real-time applications as other services, such as mass file transfers or streaming video, consume the majority of available bandwidth. To resolve these quality issues, you, as an admin, can handle the bandwidth with QoS implementations [99]. You can refer to Chapter 3 for QoS implementation, and split-tunnel VPN implementation.

Teams Audio and Video Call Quality Issues and Dependency

Network

Optimal call quality in Teams is dependent on good network conditions. The Teams apps will highlight network connectivity issues during the call, as shown in the example in Figure 7-5, which shows poor network conditions. Use a network assessment tool to investigate network conditions and switch connectivity (e.g., wireless to wired) if possible. Expect a higher quality on a managed corporate network than on an unmanaged network like public WiFi.

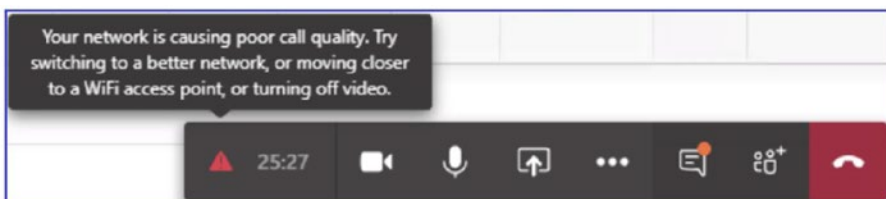


Figure 7-5. *Bad network quality in a Teams meeting*

Device

For the best audio and video quality, avoid using built-in audio devices; instead use a USB device listed at <https://products.office.com/en-us/microsoft-teams/across-devices/devices/category?devicetype=36>. These devices are certified for the best audio and video quality. Here are a few best practices for troubleshooting devices.

- If a USB device is not recognized by a computer, then connect the device to a different USB port, as the port might have an issue.
- Try connecting the device directly to the computer; avoid a USB hub for the headset or camera.
- Installing the latest device driver might remediate some audio and video quality issues. The use of a headset on the microphone/line-in port of your computer is not a suitable replacement for a USB device, as these devices are dependent on the computer's audio devices, as well.
- Using a USB headset (headphones) prevents your microphone from picking up audio from your computer or background noise. Sometimes the sound is amplified and passed in and out frequently, resulting in an unpleasant, loud static or scream. Remember using a headset helps to eliminate sources of echo as well.
- If you are unable to use a headset, try to put as much distance as possible between your speakers and microphone to minimize any background noise.
- If you are planning to use a built-in audio device (considering the previously mentioned problems), set up your audio device correctly to manage your Windows audio device.
 - a. First search Manage Audio Devices. Select Recording and then select the playback device (headset) that you want to set as default for Teams as well as the computer. For example, in Figure 7-6, I selected Microphone Array (Realtek High Definition Audio).

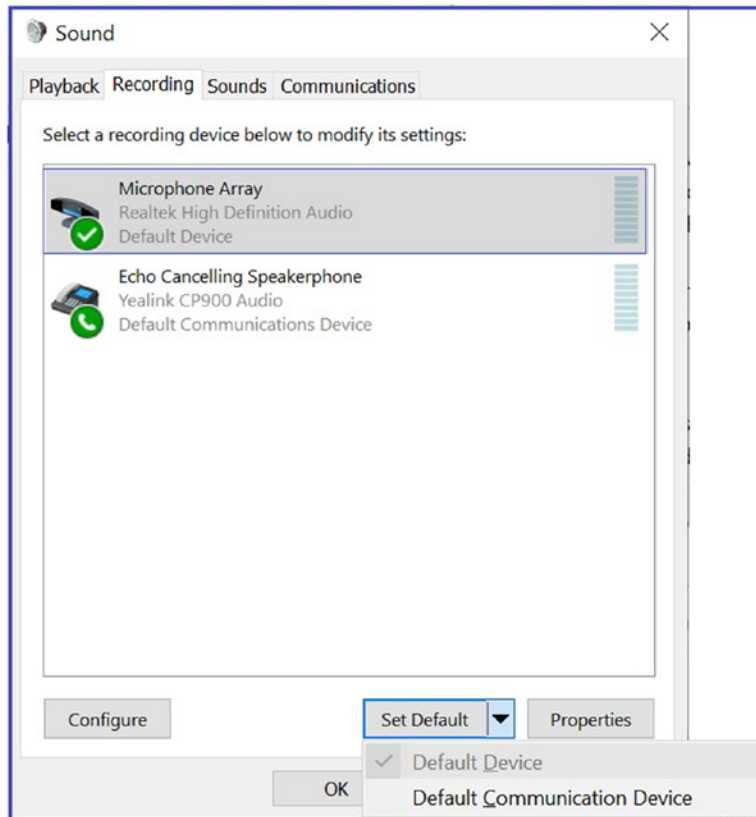


Figure 7-6. Select a device and setting it as the default

- b. Click Properties to set advanced options. Select the Enhancements tab and then select the Acoustic Echo Cancellation (AEC) and Far Field Pickup (FFP) check boxes, as shown in the Figure 7-7.

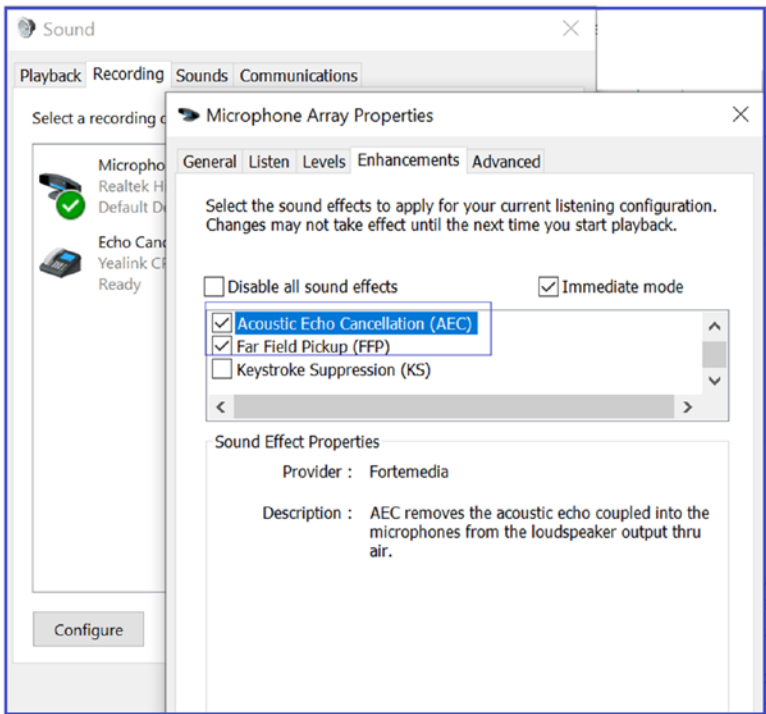


Figure 7-7. Properties for a recording device

How Teams Audio and Video Calls Work

Teams allows one-to-one audio and video calls as well as multiparty meetings. First, understand how a one-to-one audio and video call works. For example, user Balu is calling user Chanda. Teams clients always send their chat service (signaling) traffic to Teams service (Office 365 cloud) over 443/TCP. Refer to <https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#skype-for-business-online-and-microsoft-teams> for port numbers and FQDNs used by Teams.

Teams audio/video and desktop sharing media traffic will prefer a direct connection over UDP. Teams prefer the most direct connection possible. To establish a connection in Teams, leverage the Interactive Connectivity Establishment (ICE) protocol to find the most optimal path to send media. In the example shown in Figure 7-8, direct connectivity between user Balu’s computer and user Chanda's computer is possible, and both clients send media directly between them.

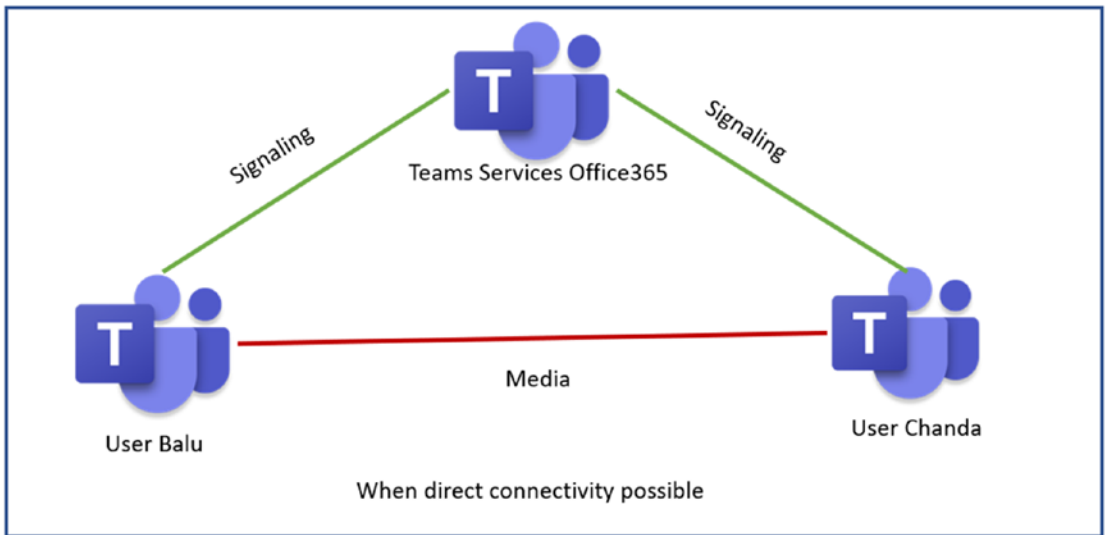


Figure 7-8. Teams direct audio/video call

If direct connectivity isn't possible because of a firewall between two endpoints, chat and content still go directly to the Teams service (Office 365 cloud) via 443 (most organizations always allow 443). This way, they can then exchange private chat, files, and so on. They also contribute to the same channels; as you can see in Figure 7-9, the firewall between them is not a problem for signaling traffic.

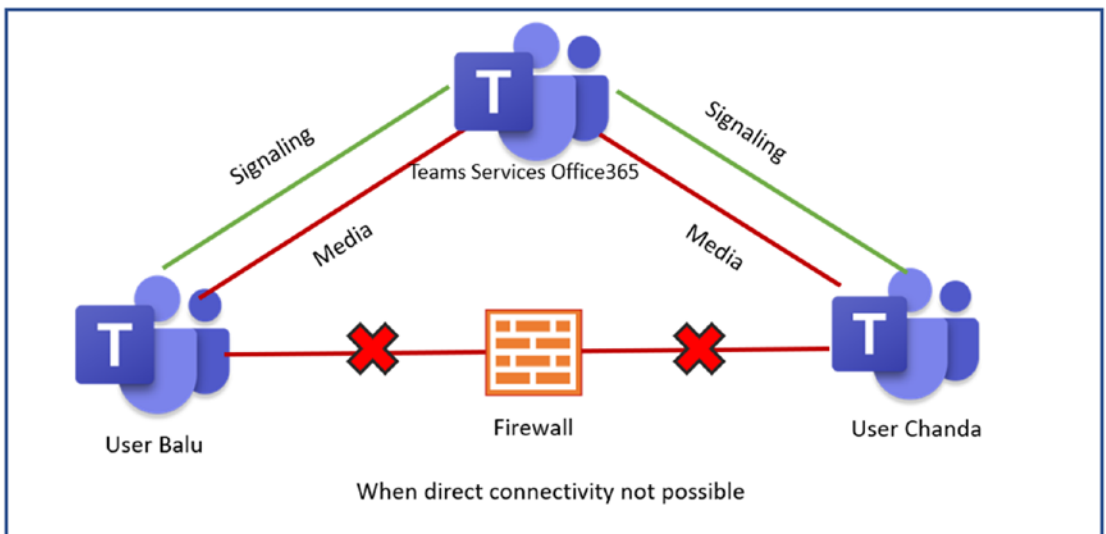


Figure 7-9. Teams audio/video call via relay

However, when they start the audio/video real-time session, the firewall blocks their traffic because a direct connection is not possible. In this situation, Teams uses a relay. Basically, user Balu will establish a connection with Office 365, and user Chanda will also establish a connection with Office 365 for this session. Office 365 Relay will proxy any real-time traffic to another relay to another user. User Balu and user Chanda can talk to each other even though there is no direct connectivity. Office 365 functions as a relay for the media traffic, if direct connections are not possible. This media path is not optimal because all client traffic has to go to the Office 365 relay first and then to other users, so this will affect latency and network jitter, but at least Teams allows audio and video instead of no call, which is important.

Teams always preferred UDP with port 3478 to 3481. What if UDP is not available? In that case, Teams can be failed back to TCP with 443, and the call will work, but call quality will not be optimal.

There are some built-in tools in the Teams service that help you identify a call quality problem. For any issue, without identifying it you cannot resolve it. Teams provide two tools, Call Analytics and Call Quality Dashboard (CQD) to use when you encounter call quality problems.

Call Analytics

This is my favorite tool, and I frequently use this when I troubleshoot individual users' call quality issues. Call Analytics provides detailed information about the user of the device connected, networks (internal or external, wired or wireless), and connectivity related to specific calls and meetings for each user in a Microsoft Teams or Skype for Business account. You, as an admin, can use Call Analytics to troubleshoot call quality and connection problems experienced in a specific call or meeting using Teams admin center.

To access Call Analytics that can help you to identify and eliminate problems, follow these steps.

1. Log in to the Teams admin center and navigate to Users. Find the user who encountered a problem and then select that user to open the user's account properties.
2. Click Call History, which will show the detailed call history for the user, including the last seven days of call quality and activity data. Call history shows one-to-one calls and meeting audio quality. Figure 7-10 is a sample user call history.

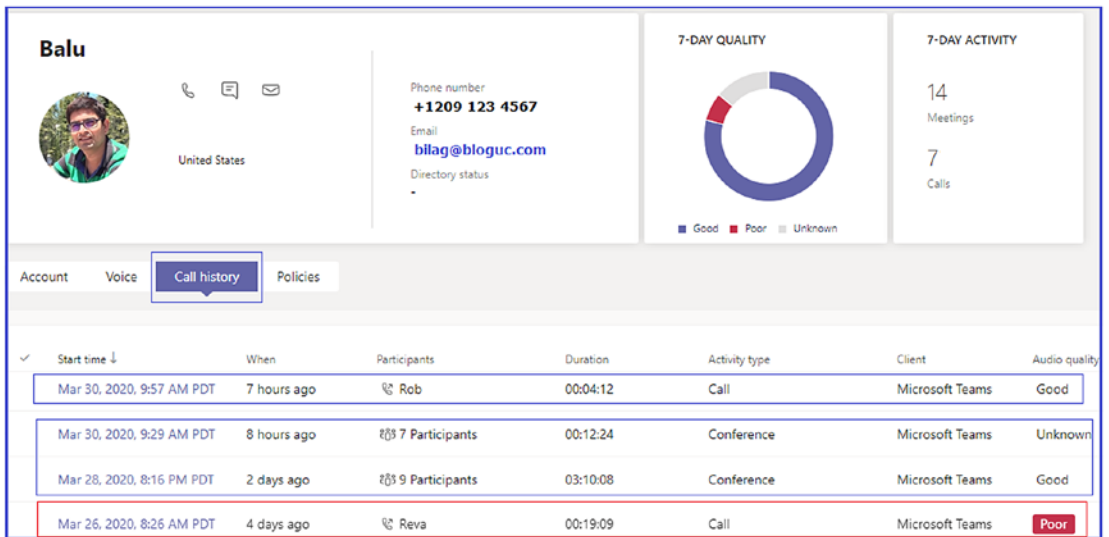


Figure 7-10. Call Analytics

- When you select a particular meeting or call, you will see the call quality details, including device, system, connectivity, and network details. For example, in the example shown in Figure 7-11, I selected a call between Balu and Reva, which was marked as having poor audio quality. Clicking on Network, it shows the average packet loss was over 14 percent, which is very high, and the maximum packet loss rate was over 25 percent, which is why the audio quality is marked as poor. The statistics also include network quality, including RTT (latency), jitter, and packet loss.

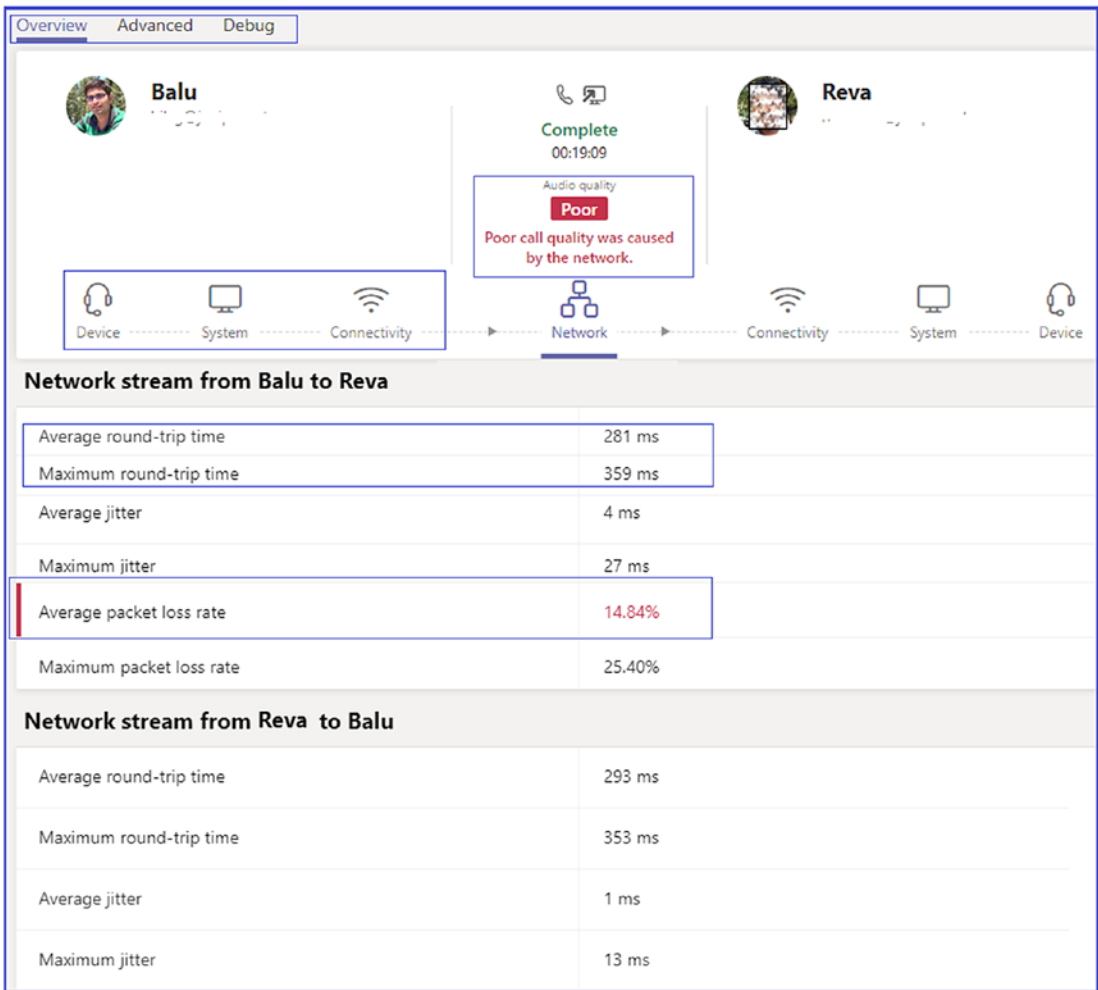


Figure 7-11. One-to-one call network statistics

4. If you are interested in doing a deeper dive, then click the Advanced tab or Debug tabs, which show more details on what IP address was used, protocol, and port used for the media session.

Microsoft Call Quality Dashboard

CQD is designed to help Teams admins and network engineers optimize their overall network. You cannot analyze and troubleshoot a single call using CQD. It allows us instead to look at combined information for an entire organization. This can also help you to identify and reduce problems that are on the whole site or network. Figure 7-12 shows the overall audio quality for Bloguc Inc. You can access CQD in two ways.

- You can log in to the Teams admin center and then select Call Quality Dashboard. Click Sign In to access overall call quality and summary.
- Alternatively, you can directly visit <https://cqd.teams.microsoft.com/> and log in to access CQD. Figure 7-12 shows a display of monthly and daily Teams audio trends.

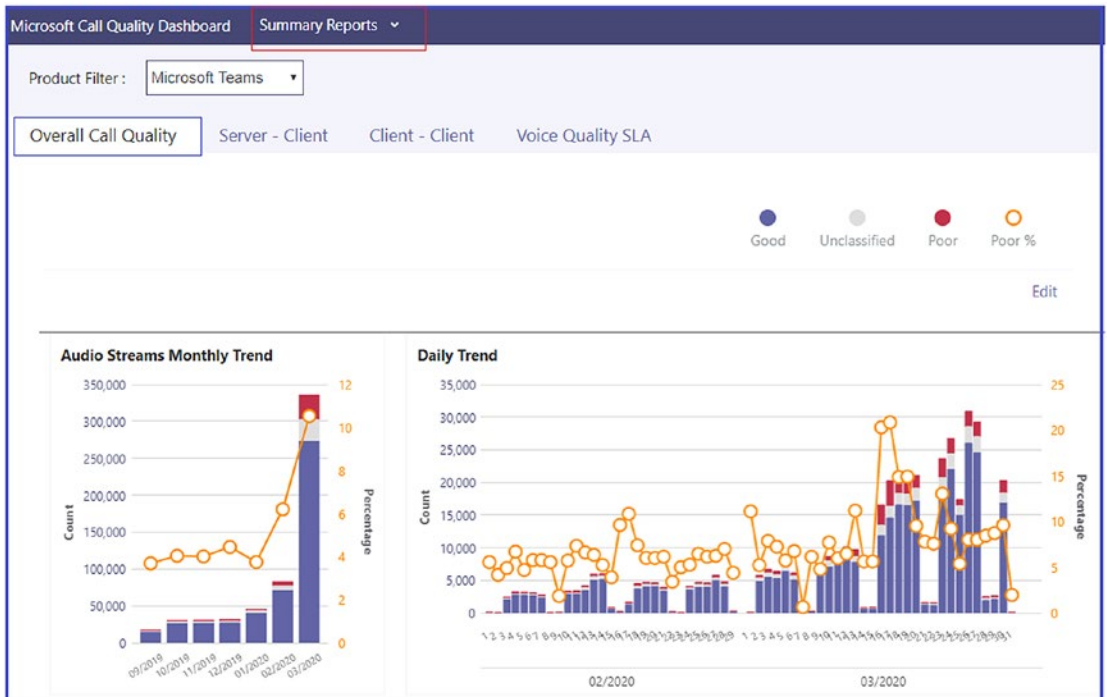


Figure 7-12. CQD displaying overall call quality

Teams Phone System (PSTN) Call Troubleshooting

Microsoft Teams only supports E.164 format numbers, so make sure to configure E.164 format phone numbers.

Customizing Call Features in Teams Client

In Teams client, you can configure how you want to handle incoming calls. To do so, log in to the Teams (desktop) client and then click your profile picture. Click settings and then click Calls, In to configure how you want to handle calls. You might want to ring

calls to your Teams client, or you might want to forward phone calls to a different phone number. Here are the options.

1. When you select the Calls Ring Me option, you can also choose the Also Ring option to simultaneously ring another phone number.
2. Select If Unanswered, then select Send To Voicemail, Another Number Or Call Group, or Do Nothing, which is the default.
3. If you opt to redirect to another number, then enter after how what period you want to redirect this call. The example in Figure 7-13 shows 20 seconds, which is the default.

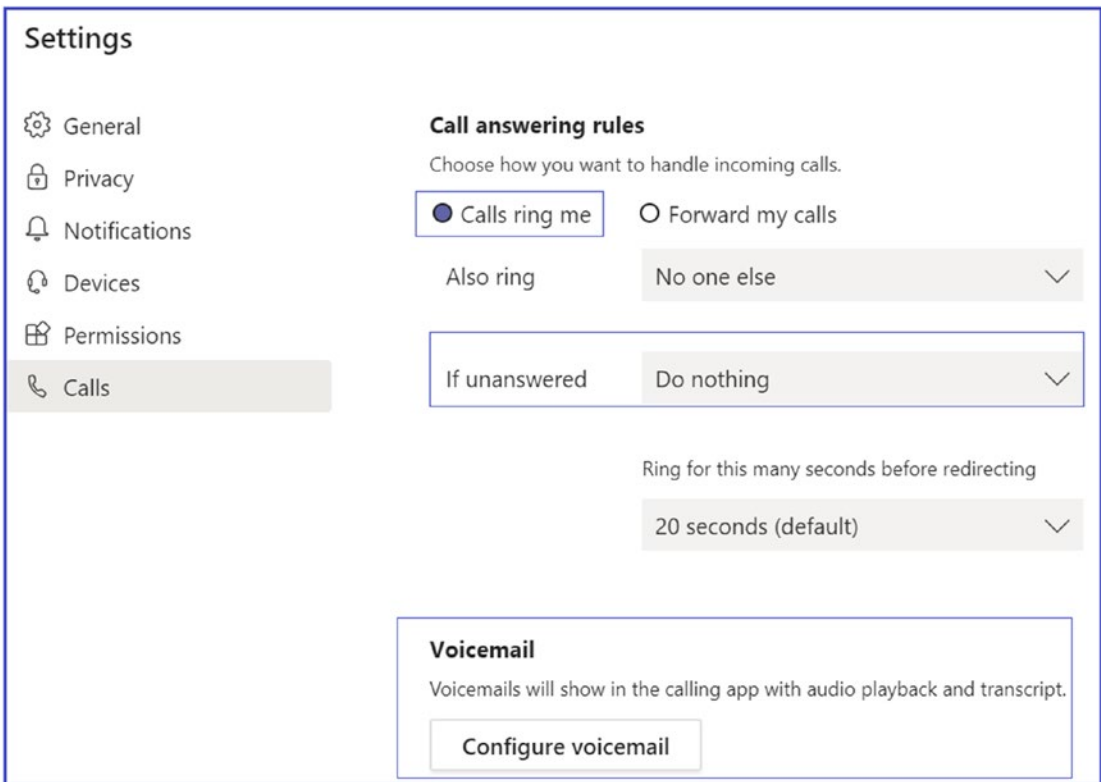


Figure 7-13. Call answering options

All these features matter for the user experience and the settings quite self-explanatory.

Phone Dial-Pad Is Missing in Teams

In Teams, if a dial-pad is missing, users cannot make outbound calls (user can receive inbound calls). There are some prerequisites that need to be fulfilled to have a phone dial-pad in the Teams client. Ensure the following things are in place to use a phone dial-pad in Teams.

1. Users must have a valid Teams Phone System (Microsoft 365 Phone System) license assigned.
2. Users should have enterprise voice enabled. If not, then run this PowerShell command to enable the user for enterprise voice in Teams.

```
Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

3. If you are using Teams Direct Routing, then make sure users have an OnpremiseLineURI number assigned or Microsoft Calling Plan and online phone number assigned to the user.
4. To work with outbound calls assign a voice routing policy with proper PSTN usage and routes.

Troubleshooting Call Failures with Call Analytics

Whenever Teams client attempts a phone call, it captures some call quality and diagnostics information. That information is used by the Teams service and analyzed by Teams Call Analytics. Teams Call Analytics is the best tool to check call failures.

To access Call Analytics, you must have the appropriate permissions. To access Call Analytics, log in to Teams admin center, navigate to Users, and then find the user you want to access. Once the user page opens, click Call History and then find the PSTN call that has a problem. For example, Figure 7-14 shows a short call that has an issue.

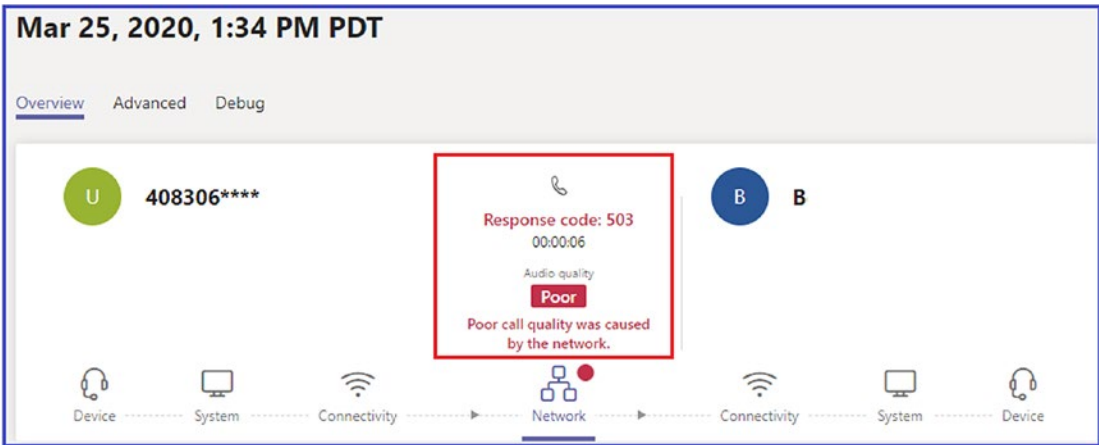


Figure 7-14. Teams PSTN call

There are different call failures and codes you might see in Call Analytics such as Response code 486, Response code 408, Failed destination does not exist, 404 not found, and so on.

Unable to Connect to Voicemail in Teams

If you are unable to connect to voicemail using the Teams client, then the first thing you can do is download the Teams diagnostics log. For Windows, press Ctrl+Alt+Shift+1; for macOSX, use Command+Option+Shift+1. Open the downloaded log file and search for Voicemail-List, then review any ERR messages. That is your signal to troubleshoot the issue further.

If You Are Unable to Connect to Exchange, Then Teams and Outlook Connectivity Breaks

Understand that Microsoft Teams is tightly integrated with Exchange (Outlook), and if there is an issue, then Teams and Outlook connectivity will be broken. Check that Outlook is connecting, and check user credentials.

Restoring a Deleted Channel

A team owner can restore a deleted channel. To restore a deleted channel, navigate to Teams and then next to the team's name, click More Options (...) and select Manage Channel. Click the Channels tab and then expand the Deleted section. Click Restore, as shown in Figure 7-15.

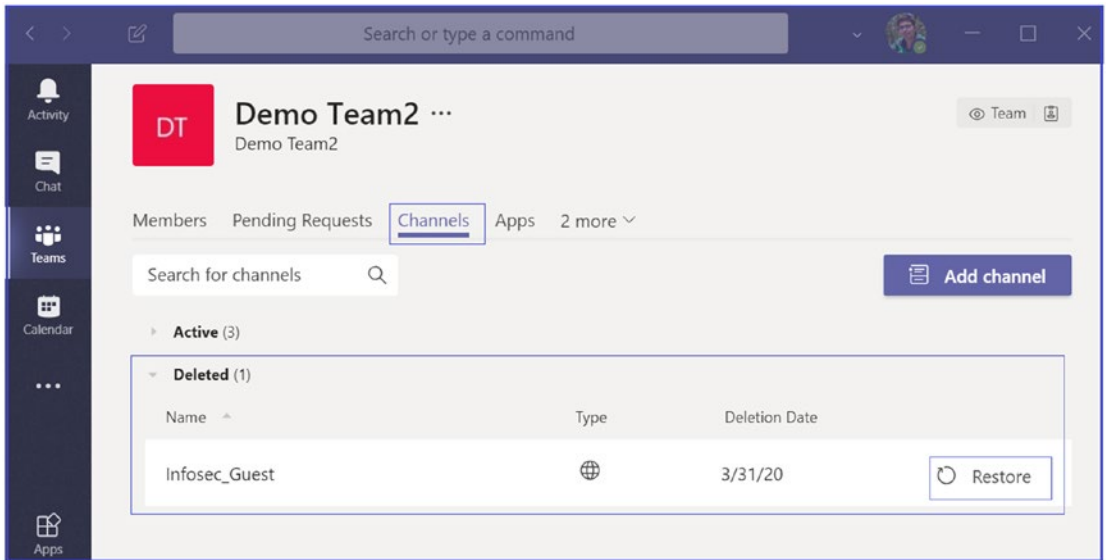


Figure 7-15. Restoring a deleted channel

Available Tools for Effective Troubleshooting

Microsoft Teams is dependent on different Office 365 services, such as SharePoint Online, Exchange Online, Skype next-gen, OneDrive for Business, and so on. Therefore, if a dependent service fails, it directly affects Teams performance. This makes checking Teams service health, network connectivity, and performance very important.

Verifying Teams Service Health Using Health Tool

Microsoft has provided Service Health, Message center, and Directory Sync status subtools to validate Teams' overall health. Service Health for Microsoft Teams is available on the Office 365 Admin portal main page. It is highly recommended to check

and validate Teams and through Service Health frequently. When you encounter a Teams service issue, before doing any further troubleshooting for that issue, you should confirm that the Teams service is healthy.

Microsoft Teams is built on top of Office 365 services, so when checking Service Health, consider checking the status of Exchange, SharePoint, and OneDrive for Business. Service Health issues for these other services do not automatically mean that Teams is affected (e.g., Address Book downloads in Exchange are unavailable), but you should review the advisories for those affected services to determine if there is an impact to Microsoft Teams [100].

Microsoft is continually adding service improvements and feature updates to Teams; therefore, as an admin, you must keep an eye on Microsoft notifications, alerts, and official documentation. You will get a notification, message, or alert when there is any service degradation. Therefore, keeping an eye on Message center is critical, and one of the tasks that admins must do daily. To access Message center, you need to visit the Office 365 admin center, navigate to Health, and then select Message Center, as shown in Figure 7-16.

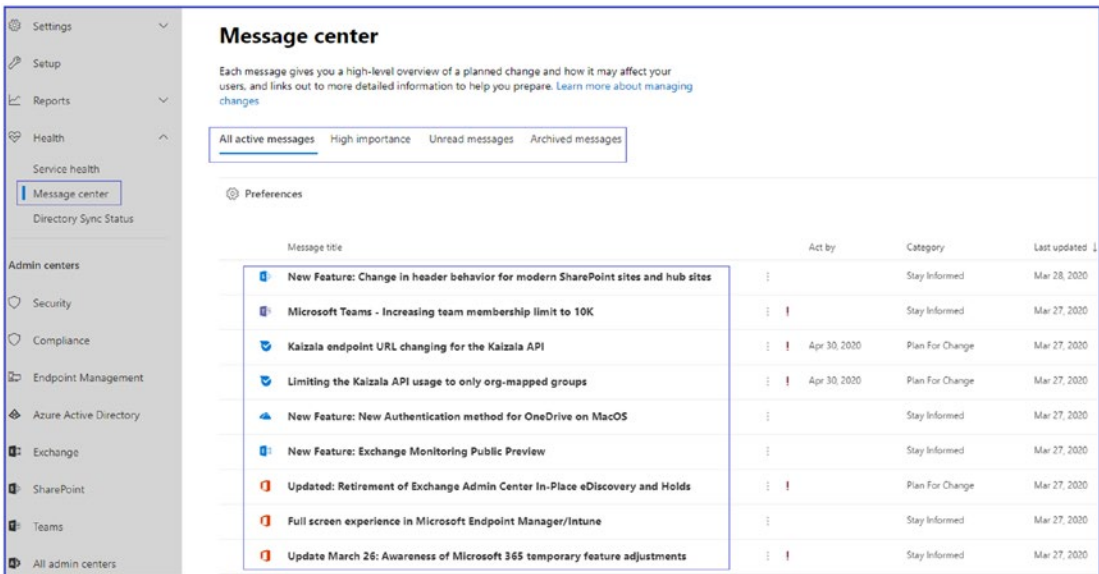


Figure 7-16. Message center showing active and unread messages

Checking Teams Service Health

Frequently checking the health of Teams and dependent services is highly recommended. You can automate service health notification by setting email, so whenever service degradation happens, you will receive an email alert. To set an email for notification, log in to Teams admin center and navigate to Health. Select Service Health, and then click Preferences. In the Preferences window, add two email addresses that can receive a proactive notification via email, as shown in Figure 7-17.

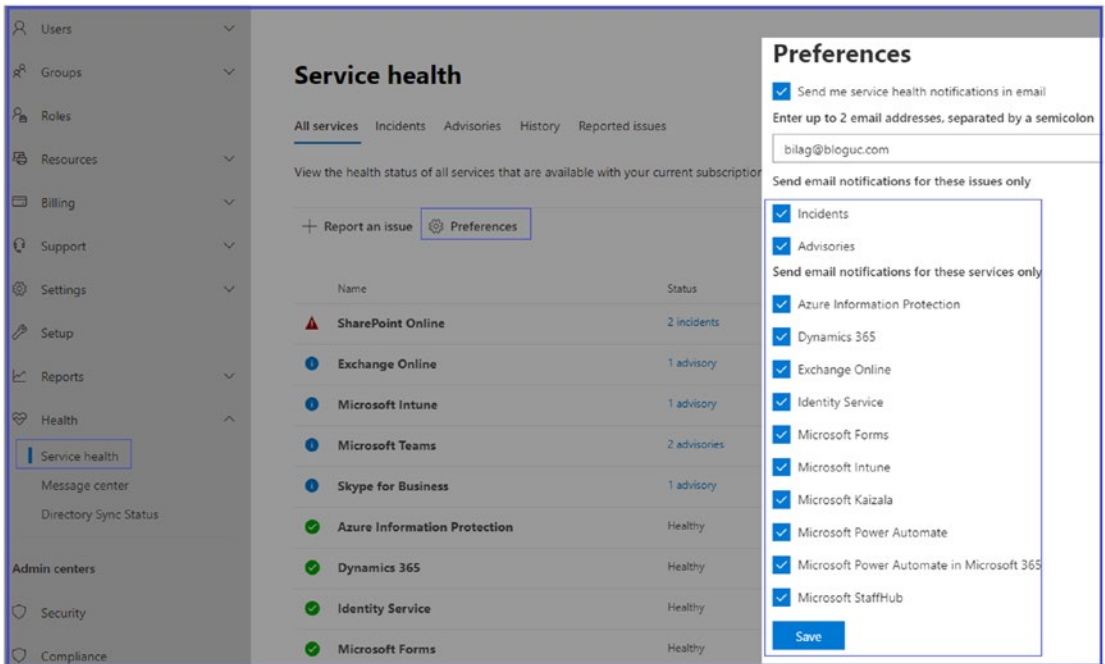


Figure 7-17. Service Health email notification settings

Once you add a new email address or change the existing email address, it could take up to 8 hours for these changes to take effect. Sometimes it can take up to 12 hours to apply a policy, although in general they take an hour. Microsoft has a 24-hour SLA for any policy changes to apply because the Teams service resides in Office 365 cloud, and user objects might be on-premises.

Microsoft Teams Network Assessment Tool

When a user reports Teams call connectivity and quality issues, you can use this network assessment tool, which helps to test network quality and connectivity from users' locations to Teams media services.

The network assessment tool is very helpful to test network quality. This assessment tool analyzes the connection to Microsoft Network Edge (pairing point) by running a set of packets to the closest edge site and back for approximately 20 seconds for a configured number of iterations.

Types of Test

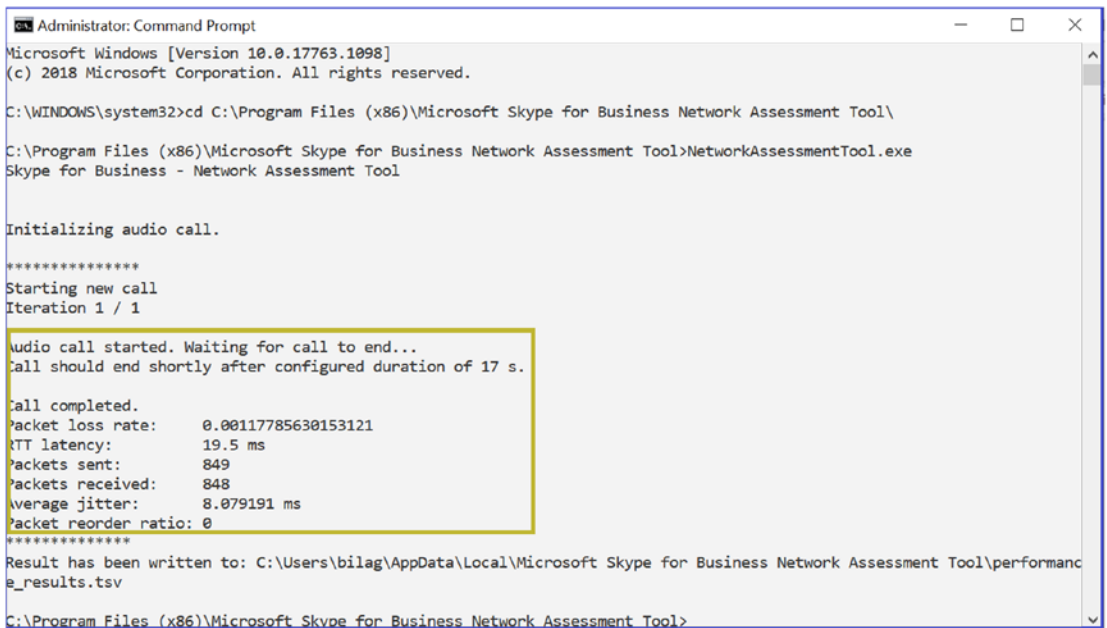
This tool is named Skype for Business Network assessment tool; however, it is applicable for both Skype for Business and Microsoft Teams. You can run this tool on Windows 8 or newer operating systems. It helps test network connectivity as well as network performance.

- *For network connectivity:* This tool verifies the network and network elements between the test location and the Microsoft network are correctly configured to enable communication to the IP addresses and ports (using UDP and TCP) needed for Microsoft Teams calls. The addresses and ports are listed at https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2#bkmk_teams.
- *For network performance:* To check the network, this tool tests the connection to Microsoft Network Edge by running audio packets to the nearest edge site and back for approximately 17 seconds for a configured number of iterations. The tool collects packet loss, jitter, round-trip latency, and packet reorder percentage from each call. The results from a set of test calls can be analyzed to determine if it meets the media quality and performance targets described at <https://support.office.com/en-us/article/Media-Quality-and-Network-Connectivity-Performance-in-Skype-for-Business-Online-5fe3e01b-34cf-44e0-b897-b0b2a83f0917>. These targets and testing applications are for both Microsoft Teams and Skype for Business Online calls.

Using the Network Assessment Tool

First, download this tool by visiting the Microsoft site at <https://www.microsoft.com/en-us/download/details.aspx?id=53885>, and then install the executable file. It typically installs in C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool. Once it is installed, open a command prompt run as administrator and then go to the path where the network assessment tool installed. Run NetworkAssessmentTool.exe. Once it runs, it initializes the audio call and shows detailed results with packet loss, jitter, latency, packet reordering, and so on, as displayed in Figure 7-18. Use this sample command.

```
c:\Program Files\Microsoft Skype for Business Network Assessment
Tool>NetworkAssessmentTool.exe
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool\

C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool>NetworkAssessmentTool.exe
Skype for Business - Network Assessment Tool

Initializing audio call.

*****
Starting new call
Iteration 1 / 1

Audio call started. Waiting for call to end...
Call should end shortly after configured duration of 17 s.

Call completed.
Packet loss rate: 0.00117785630153121
RTT latency: 19.5 ms
Packets sent: 849
Packets received: 848
Average jitter: 8.079191 ms
Packet reorder ratio: 0
*****
Result has been written to: C:\Users\bilag\AppData\Local\Microsoft Skype for Business Network Assessment Tool\performance_results.tsv

C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool>
```

Figure 7-18. Network assessment tool

Another test you can perform is the connectivity checks test for all of the IP addresses and ports used in Microsoft Teams calls or meetings. Figure 7-19 shows the connectivity test result with HTTPS, TCP, and UDP; ports, and all IP addresses used by Microsoft Teams and Skype for Business Online. You can use the following parameter to do connectivity checks.

```
c:\Program Files\Microsoft Skype for Business Network Assessment  
Tool>NetworkAssessmentTool.exe /connectivity check /verbose
```

Figure 7-19 shows Teams and Skype for Business Online IP addresses and ports are reachable.

```
C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool>NetworkAssessmentTool.exe /connectivitycheck /verbose  
Skype for Business - Network Assessment Tool  
  
Starting Connectivity checks  
Relay : 13.107.64.2 is reachable using Protocol UDP and Port 3478  
Relay : 13.107.64.2 is reachable using Protocol TCP and Port 443  
Relay : 13.107.64.2 is reachable using Protocol HTTPS and Port 443  
Relay : 13.107.65.5 is reachable using Protocol UDP and Port 3478  
Relay : 13.107.65.5 is reachable using Protocol TCP and Port 443  
Relay : 13.107.65.5 is reachable using Protocol HTTPS and Port 443  
Relay : 52.113.192.2 is reachable using Protocol UDP and Port 3478  
Relay : 52.113.192.2 is reachable using Protocol TCP and Port 443  
Relay : 52.113.192.2 is reachable using Protocol HTTPS and Port 443  
Relay : 52.113.193.5 is reachable using Protocol UDP and Port 3478  
Relay : 52.113.193.5 is reachable using Protocol TCP and Port 443  
Relay : 52.113.193.5 is reachable using Protocol HTTPS and Port 443  
Relay : 52.114.188.1 is reachable using Protocol UDP and Port 3478  
Relay : 52.114.188.1 is reachable using Protocol TCP and Port 443  
Relay : 52.114.188.1 is reachable using Protocol HTTPS and Port 443  
Relay : 52.114.188.254 is reachable using Protocol UDP and Port 3478  
Relay : 52.114.188.254 is reachable using Protocol TCP and Port 443  
Relay : 52.114.188.254 is reachable using Protocol HTTPS and Port 443  
Relay : 52.114.189.1 is reachable using Protocol UDP and Port 3478  
Relay : 52.114.189.1 is reachable using Protocol TCP and Port 443  
Relay : 52.114.189.1 is reachable using Protocol HTTPS and Port 443  
Relay : 52.114.189.254 is reachable using Protocol UDP and Port 3478  
Relay : 52.114.189.254 is reachable using Protocol TCP and Port 443  
Relay : 52.114.63.254 is reachable using Protocol UDP and Port 3478  
Relay : 52.114.63.254 is reachable using Protocol TCP and Port 443  
Relay : 52.114.63.254 is reachable using Protocol HTTPS and Port 443  
Verifications completed successfully  
  
result has been written to: C:\Users\bilag\AppData\Local\Microsoft Skype for Business Network Assessment Tool\connectivity_results.txt
```

Figure 7-19. Network connectivity checks

SIP Tester

SIP tester for Direct Routing is a PowerShell script tool that allows testing of Direct Routing SBC connections in Teams. Testing Direct Routing is quite complicated, but using the SIP tester tool makes it easier. This tool allows us to test the basic functionality of a customer-paired Session Initiation Protocol (SIP) trunk with Direct Routing, such as outbound and inbound calls, simultaneous ring, media escalation, and consultative transfer.

This SIP tester tool provides the ability to test real accounts in a Teams organization’s indirect routing scenarios. Microsoft has written a web service that tests the Teams client login against one configured with SBC Direct Routing. You can automate this PowerShell script to make daily calls and checks to determine if SBC is working correctly or not.

To download the SIP tester tool, visit the Microsoft site at <https://docs.microsoft.com/en-us/microsoftteams/sip-tester-powershell-script>.

You can read further documents that come along with a script to understand the requirement to create test users, which will be used for basic call testing scenarios.

Refer to my blog at <https://bloguc.com> for more Teams client service troubleshooting information and best practice guidance.

Summary

Microsoft Teams is a unified communication and collaboration tool that works very well when your environment is prepared in advance, such as allowing Teams services, IP addresses, ports and protocols, URLs, and FQDNs from your corporate firewall so that each Teams feature works correctly. As part of troubleshooting, you should identify and use the core tools for Microsoft Teams, namely Call Analytics and CQD. You can also collect diagnostic information from Teams clients, troubleshoot common Teams problems, and more.

It is also important to use the right tool, and knowing when to use them will help to effectively make progress when identifying and troubleshooting Teams problems that users might encounter. Some of these helpful tools are Teams Call Analytics, CQD, and the network assessment tool described in this chapter.

CHAPTER 8

Take Your Learning to the Next Level

Wow! You reached the last chapter! You did a commendable job reading through the previous seven chapters. This chapter mainly covers managing Microsoft Teams certification planning and preparation details.

Now that you have invested your valuable time in reading and learning about Microsoft Teams administration, it is beneficial to take all your learning to the next level by earning certification. The inspiration for me to write this chapter is to provide you with brief details on planning and preparation for the Managing Microsoft Teams certification exam so that you can realize success in your learning journey. Let's read this chapter and get ready for the Managing Microsoft Teams (MMT) - MS 700 exam; once you pass you will earn the certification Microsoft 365 Certified: Teams Administrator Associate.

Microsoft Teams Administrator is a relatively new role, but existing Skype for Business (Lync), Telecom admin, Unified communication and collaboration admins, and Support admins also qualify for the Teams administrator role. This role is quite vast and involves multiple responsibilities, such as configuring Teams settings and policies, deploying and administering client software, and managing Office 365 workloads for Microsoft Teams that focus on practical and efficient collaboration and communication in an enterprise environment. If you qualify for the Teams administrator role, then you must be able to plan, deploy, adapt, communicate, and manage all team features. An admin in this role is also accountable for upgrading user workload from Skype for Business to Microsoft Teams and must be acquainted with telephony integration and Teams Phone System Direct Routing using SBC and Teams Phone System Calling Plan and Teams Audio (dial-in) Conferencing [101].

Apart from planning, deployment, and administration, you have to collaborate with telephony engineers to integrate advanced voice features into Microsoft Teams, including but not limited to configuring Teams Direct Routing using SBC, integrating telephony, phone number (DID) porting, number translation, voice gateway for analog devices, and so on. You might work with other workload administrator roles, including security and compliance admins, messaging admins, networking engineers, identity management admins, and audio/video device admins.

Before taking the Managing Microsoft Teams certification exam, you must understand the different components of Teams, and Teams chat, calls, meetings, teams and channels, app policies, and overall Teams administration using Teams admin center and Windows PowerShell. Most important, you must be familiar with managing Teams policy settings by using Teams admin center as well as PowerShell. Apart from Teams knowledge, you must have a basic understanding of integration points with apps and services, including but not limited to SharePoint, OneDrive for Business, Exchange Online, Azure AD, and Office 365 Groups (see Chapters 1 and 2).

Planning and Preparing for the Managing Microsoft Teams Exam

Understanding the Exam Structure for Managing Microsoft Teams (MS-700)

You must attempt all questions on the exam, as there is no negative marking for the Managing Microsoft Teams exam. You will have 180 minutes to attempt 40 to 60 questions; some questions might be worth more than one point. You must plan your time wisely, with 150 minutes to answer questions and an additional 30 minutes for instructions, comments, score reporting, and so on.

The exam will likely include a case study based on the detailed information on business and technical requirements, existing environment, and other background information you need to solve problems using simulation. Also, you need to understand and integrate information across multiple sources, determine what is essential, and make the best decision.

Exam Summary

Remember, this is not a training course, nor does this book provide everything you need to know to pass the exam. Still, this book will provide you with detailed information that is required to pass this exam. The exam is divided into three main sections. The first part is the plan, and it configures a Microsoft Teams environment. This section accounts for up to 45 to 50 percent of the exam questions. The second section is on managed chat, calling, and meetings, which will have about 30 to 35 percent of the exam questions. The last section tests managing Teams and app policies, which will make up 20 to 25 percent of the exam questions.

The first section is more about how you need to prepare your environment before you deploy Microsoft Teams, including migration from Skype for Business to Teams, planning and configuring network settings for Microsoft Teams, implementing governance and life cycle management for Microsoft Teams, configuring and managing guest access, managing security and compliance, deploying and managing Microsoft Teams endpoints, and finally monitoring and analyzing service usage [101].

This chapter covers each topic that you learned as part of Teams administration, but not in great detail.

Section 1: Plan and Configure a Microsoft Teams Environment

This section covers overall Teams deployment planning and preparation and configuration in brief detail. If you want to understand each topic in depth, you need to review the relevant chapters earlier in the book. This section of the exam includes the most questions (between 45 and 50 percent). I recommend spending more time on this section to get familiar with each topic mentioned here. Also, review the previous chapters to get comfortable the topic of configuration.

- Upgrade from Skype for Business to Microsoft Teams.
- Plan and configure network settings for Microsoft Teams.
- Implement Governance and Life Cycle Management for Microsoft Teams.
- Configure and manage guest access.
- Manage security and compliance.

- Deploy and manage Microsoft Teams endpoints.
- Monitor and analyze service usage.

Upgrade from Skype for Business to Microsoft Teams

If your organization has a Skype for Business environment, the very first thing you need to do is think about the upgrade path from Skype for Business to Microsoft Teams and then understand the five coexistence modes. Choose the coexistence mode that will best meet your organizational requirements.

Start an upgrade path with a small group of users; ideally, you can choose IT organization users who understand things and can test things better for you, and then gradually expand to the whole organization. I would recommend planning an upgrade by region. Migrating users in the same region, on the same Teams mode, works better. If you move half of the users from North America and half from the Asia-Pacific region, then the remaining users will not have a similar experience, causing more confusion. For that simple reason, a region-wide or site-wide approach works better.

You need to select an appropriate upgrade path and coexistence mode to meet your organization's specific needs and requirements. When you migrate pilot users to Teams, they might see issues involving their existing meetings not being migrated to Teams. As an admin, you need to plan to check meeting migration status and troubleshoot meeting migration requests, in case there is an issue. Microsoft has provided Meetings Migration Service (MMS). Once this service is triggered, the meetings migration process can take up to two hours until it is finalized. It could take longer if the user has many meetings.

Note If an error occurs during the migration process, MMS will periodically retry up to nine times during a period of 24 hours.

You also need to understand the user experience. This includes configuring Microsoft Teams upgrade notifications and meeting app options. At the end, you need to configure a coexistence mode for the organization and per user. Figure 8-1 shows the available coexistence modes. You should understand each mode and its details. You can review Chapter 6 for upgrade mode and migration details.

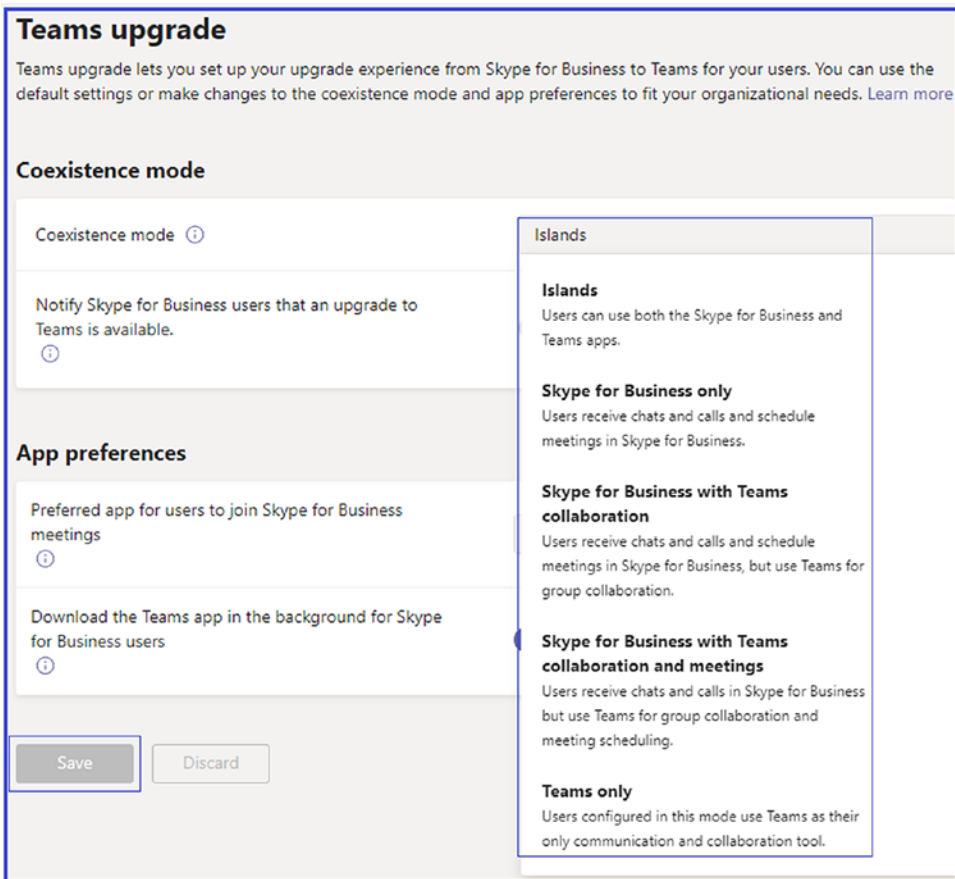


Figure 8-1. Coexistence mode

Plan and Configure Network Settings for Microsoft Teams

Configuring network settings for Microsoft Teams is another critical task that admin need to perform. Persistent chat, presence, and instant messaging will work flawlessly out of the box, but as soon as you turn on audio, video, and application sharing, that might not work as required to allow Teams traffic via a corporate firewall with optimized networking. Also, for Teams, optimal call quality requires having enough network bandwidth for audio, video, and application sharing. For example, if there are 5,000 users in the Bloguc HQ office using local Internet and local PSTN for outside phone calls, then how much network bandwidth will you be required to provide for optimal call quality in Teams? Microsoft provides a bandwidth calculator to calculate the required network bandwidth by using a network planning tool, but you must know how to use that

network planner to calculate network bandwidth capacity for Teams audio, video calls, meetings, and significant events. Basically, the network planner will estimate required network bandwidth for the specified number of users.

Another critical area is allowing Teams signaling and media traffic from your organization to Teams Office 365 cloud services. Teams do have multiple service IP subnets, service URLs and FQDNs, and wildcard URLs with require ports and protocols allowed through your organization network firewalls. It is crucial to perform network assessment. Microsoft makes this easier by providing the Network Testing Companion tool for Microsoft Teams and Skype for Business online environments. This tool makes a call and tries to establish a connection by checking the Teams service IP address through establishing connectivity tests. The tool also captures user details like how much packet loss is observed and how much jitter and latency are observed when the network connection is established [101].

In addition to allowing Teams traffic and assessing bandwidth requirements, implement QoS. Basically, Teams media traffic is audio, video, and application sharing traffic, which is latency, jitter, and packet loss sensitive. Optimizing the network is therefore crucial. QoS is one way to optimize your network bandwidth. You must know where to enable QoS, though. QoS can be implemented through different methods based on different devices. Refer to Chapter 3 for details on QoS implementation. Table 8-1 shows Teams scenarios and port requirements.

Table 8-1. *Teams Scenarios and Source and Destination Ports*

Teams Scenario	Source IP/Port	Destination IP/Port
Non-real-time traffic	Teams client IP/high ports	Office 365 80 & 443 TCP
Real-time media traffic	Teams client IP 50000–50059 UDP high ports	Transport Relays 3478–3481 UDP

Implement Governance and Life Cycle Management for Microsoft Teams

Let’s assume you are an admin working for a retail organization that has 1,000 stores across the country and your organization happens to have locations with the same Teams structure. You don’t want to spend more time repeating the same steps that you follow to create a team channel manually. You can automate the team channel creation process by creating a team template.

Tip You might get similar scenarios in the exam, so reading the scenario and understanding it is an important step before answering the questions.

Based on the way and the frequency with which your users create teams in your organization, you might need to control team creation. Basically, Microsoft Teams is created based on Office 365 Groups, and you can set up policies for Office 365 Group creation to control team creation.

There are many features that you can use for team governance, such as group creation, classification, expiration, and naming policy, which allows you to undertake seamless life cycle management.

Tip Be familiar with the group, classification, expiration, and naming policies; you might get an objective or scenario type question on policy on your exam.

Also, be familiar with how to manage Teams during different life cycle management stages. For example, if a user accidentally deleted a team a week ago, is there still a way to restore the team, and how? The answer is yes. You can restore the team, as there is a 30-day soft deletion period in which a team can be restored. You could encounter such a question on the exam.

Tip You can create a classification using only Windows PowerShell.

Remember the steps for policy creation and the restore command for group restoration using PowerShell commands, as you will likely be asked questions on this topic on the exam.

First, create team templates, then set up policies for Office 365 Groups. Create and configure Office 365 Groups for Microsoft Teams classifications, expiration policy, and naming policy

To archive, restore, and delete a team, follow this procedure.

- *Office 365 Groups creation:* `.\GroupCreators.ps1 | Set-AzureADDirectorySetting`
- *Restore soft-deleted Office 365 Groups:* `Restore-AzureADMSDeletedDirectoryObject`

Tip You can create a naming policy group expiration using the Azure AD admin center.

Remember, you can only create classifications for Office 365 Groups using PowerShell.

Here is the sample PowerShell command.

```
$Template = Get-AzureADDirectorySettingTemplate
$Setting = $template.CreateDirectorySetting()
$setting["ClassificationList"] = "Low Impact, Medium Impact, High Impact"
```

Configure and Manage Guest Access

Guest access is frequently used by organization users, and it is a common feature that allows users to work with guest users (external) and add them to the team. The guest user who is from a different organization might be a partner, a vendor, and so on. As a Teams admin, I frequently use guest access when working on a project that involves an external partner in sharing a document, calling, and chatting with them.

As a Teams admin, you must know how to configure guest access in different places, including Azure AD, Microsoft 365 admin center, SharePoint, and the Teams admin center. To monitor guest usage, you should know how to use the Azure AD access review, where you can review guest access (see [Chapter 2](#)).

Tip Remember to configure guest access in different admin centers, including Azure AD, Teams admin center, Office 365 Group, and SharePoint admin center.

Be familiar with the following topics, as you might be asked scenario-type questions or settings for these configuration steps.

- First, configure guest access from the Azure AD portal to allow users to add guests.
- Then enable guest permissions in Microsoft Teams admin center; this is an organization-wide setting.
- Then configure guest access for users in Microsoft Teams.

- Configure meetings, messaging, and calling options for guests; this is another critical setting where you can allow or restrict features.
- Managing Azure AD access review for guests is an administrator tasks, not the configuration setting. However, as an admin, you must be familiar with the Azure AD access review process.
- Also, know about the guest removal process as well.

You have to use a different admin center. To enable guest access successfully. You need to enable access in Azure AD, Office 365 Groups, and Microsoft Teams admin center. Additionally, you need to allow external access in SharePoint as well.

Tip You might be asked how to enable guest access, and you will be given the names of administrative tools. You will need to pick the right tools to enable guest access.

If you want to prevent a Teams member from adding guests to a team, you need to go to Azure AD, and turn off the Member Can Invite option.

Manage Security and Compliance

Microsoft 365 provides enterprise-grade security to Teams and compliance capability, including threat protection, information protection, and security management. For example, you as a Teams admin are working in a financial institution like banking, and their users do not allow sharing of confidential data in Teams, such as account numbers, Social Security numbers, and credit card numbers. You need to find a solution. The answer is you need to apply the data loss prevention (DLP) compliance features that allow you to create a policy that can check what is shared in Teams and if the content matches the criteria. It will then delete content and show the information message.

You must know what this compliance feature does and how to apply this feature, including DLP policy, retention policy, sensitivity labels, threat management, and IB policy. You can refer to Chapter 5 for a review.

You must be familiar with the tasks mentioned next, because you might be asked to answer or configure one of the tasks. Chapter 5 provides details about these configuration activities.

- Assign Microsoft Teams admin roles and remember role names and their list of actions.
- Create and manage compliance features, including retention and sensitivity policies.
- Create security and compliance alerts for Microsoft Teams.
- Create an IB policy.
- Finally, read security reports for Microsoft Teams.

If you are interested in learning more about the different roles and their activities, refer to the Microsoft document at <https://aka.ms/teams-rbac>.

Deploy and Manage Microsoft Teams Endpoints

The Microsoft Teams app is available for desktop (Windows and macOS), mobile (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, like desk phones, conference rooms, and common area phones. Native Teams phones and conference rooms are available that you can use; however, you need to set up resource accounts for these room devices. See Chapter 2 for Teams client deployment.

Tip You must know Teams app supported platforms and how to deploy the Teams app for a different operating system platforms. You can refer to the mentioned resources.

Here is the secure link to download the Teams app: <https://teams.microsoft.com/downloads>.

- Deploy Microsoft Teams clients to devices, including Windows, VDI (Virtual Desktop), macOS, and mobile devices. Refer to the Microsoft documentation for Teams app deployment for different operating systems at <https://docs.microsoft.com/en-us/microsoftteams/get-clients>.
- Manage configuration profiles (refer to Chapter 2).

- Manage device settings and firmware (refer to Chapter 2).
- Configure Microsoft Teams rooms. Refer to the Microsoft documentation at <https://docs.microsoft.com/en-us/microsoftteams/rooms/rooms-deploy> to configure a Teams room account with prerequisites.

Tip You might encounter a question on the Teams phone profile setup, so it is essential to be familiar with the process.

To configure the profile, you need to create a profile with custom configurations, such as general setting with device lock setting, language, time and date format, daylight saving time, device settings with a display screensaver, office hours for the device, and network settings with DHCP enabled hostname, IP address, subnet mask, DNS, and gateway. Figure 8-2 shows the profile configuration settings. You must know what customization settings are available in the profile configuration.

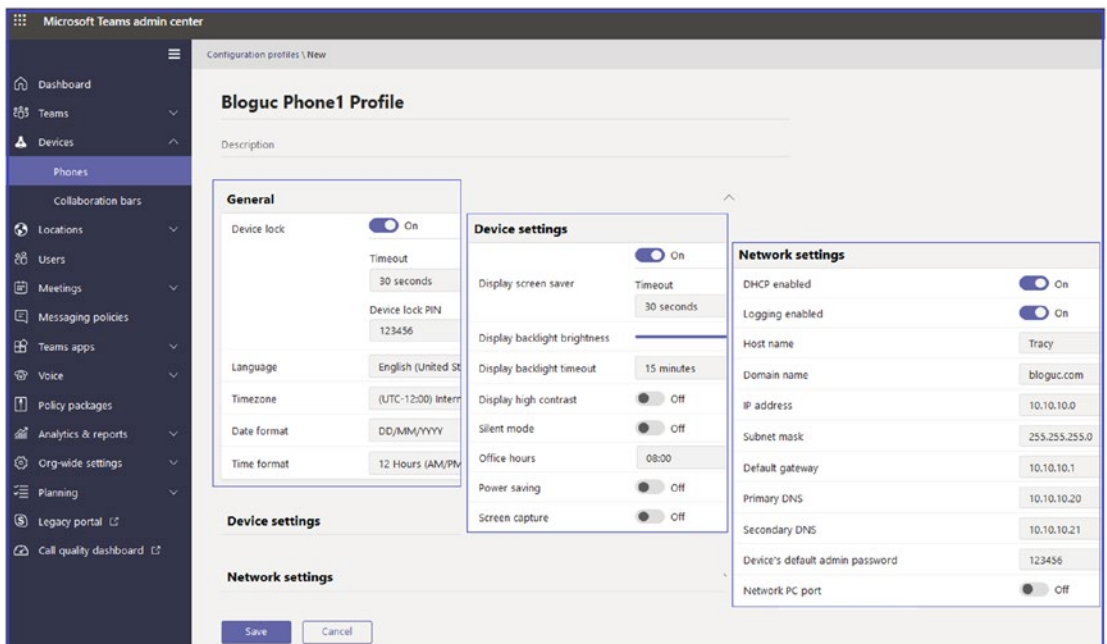


Figure 8-2. Profile configuration settings

Monitor and Analyze Service Usage

After configuring your environment and onboarding users to Microsoft Teams, you, as an admin, must analyze the services to understand the Teams adoption process as well as service usage. Microsoft has provided multiple usage reports that will help you to understand how your users are using Teams features, including teams and channels, audio and video calling, chat messages and live event, and so on.

You, as a Teams admin, must be aware of each report and understand the different usage parameters.

- Read and understand the Microsoft Teams usage reports.
- Apart from Teams usage reports, understand the Microsoft 365 usage reports.
- Comprehend Teams Call Analytics for one-to-one calls and Teams meetings.
- Analyze organization-wide call quality using the Call Quality Dashboard.

Tip You might encounter a question on the exam about how to troubleshoot individual call quality issues. The answer is to use Teams Call Analytics reports and interpret the reports to find call quality issues.

As you know, Teams is built for teamwork, so it is beneficial to check how users are using Teams, including which features they are using the most and what they are using the least. Also, Teams adoption is equally essential because the success of a Teams deployment is measured on adoption.

Microsoft has provided various dashboards and reports with the different workloads. All these reports are available through the Teams admin center. You can also compare the Teams feature usage; for example, it might show high usage on chat but low usage on calls and meetings.

You, as an admin, can analyze organization-wide call quality using the Call Quality Dashboard (CQD). Figure 8-3 shows an example of individual call analytics.

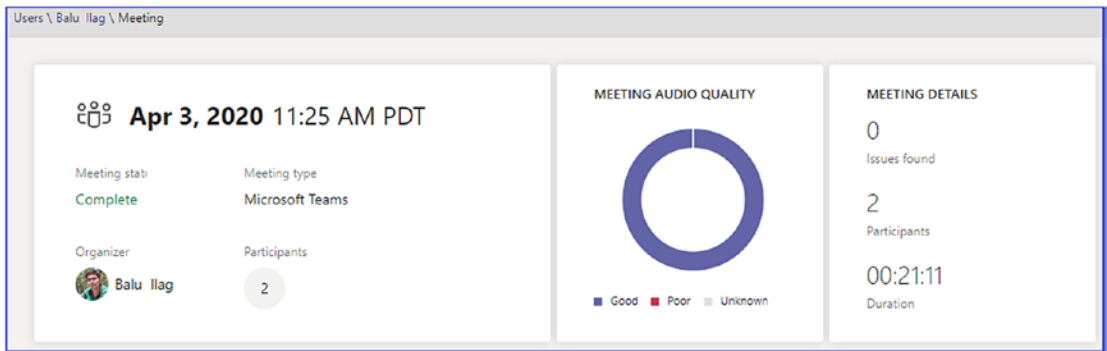


Figure 8-3. One-to-one call quality measures

Figure 8-4 shows the CQD for Bloguc Organization.

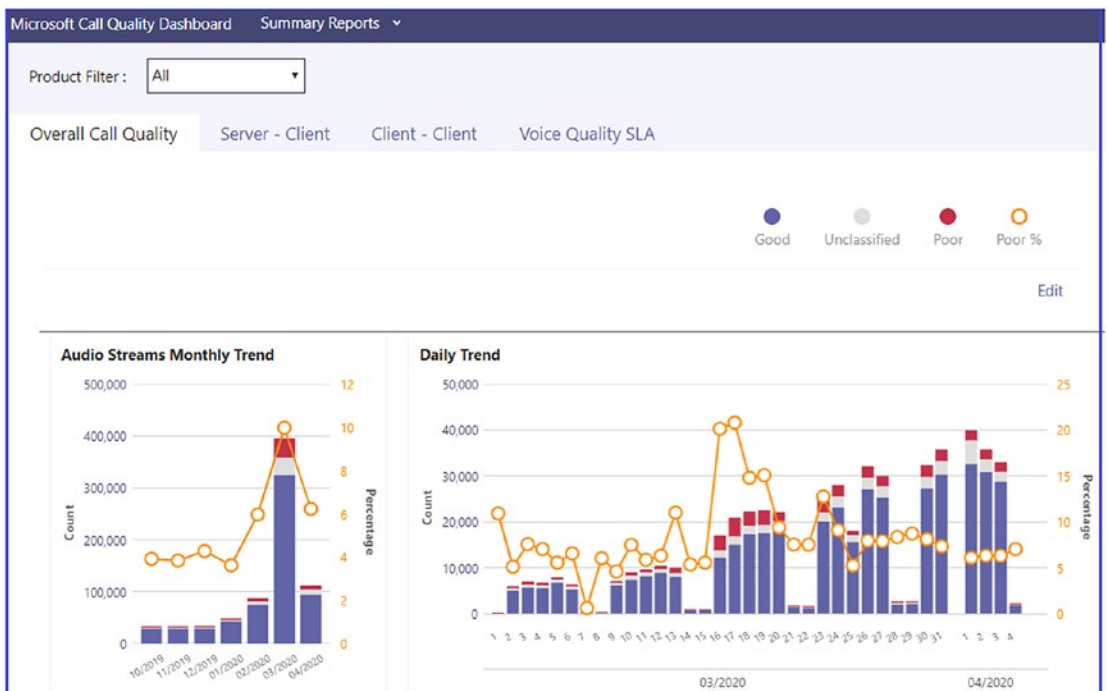


Figure 8-4. Call Quality Dashboard for Bloguc Organization

You, as an admin, can get usage reports in Microsoft 365 admin center. Microsoft Teams device usage and user activity usage reports can cover up to 180 days. If you are specifically looking for an analytics report, visit Teams Admin center, then select Analytics & Reports, and then select Usage Report. As of this writing, these reports are available for the last 7 days and the last 28 days using the Teams admin center.

Tip You might encounter a question on how to export a Teams user activity report for greater than 90 days. The answer is that you can get a Teams user activity report using Microsoft 365 admin center.

Section 2: Manage Chat, Calling, and Meetings

Microsoft Teams provides multiple capabilities to customize the user experience by allowing various settings, a policy that can be modified or changed accordingly. You can apply a different policy to a different group of users, including chat, calling, meeting, and collaboration experiences. This is another section where you will be asked questions on chat, calling, and meeting management. About 30 to 35 percent of questions or scenarios will be from this section [102].

Topics covered under this section are listed here.

- Manage chat and collaboration experiences.
- Manage meeting experiences.
- Manage phone numbers.
- Manage Phone System.

Manage Chat and Collaboration Experiences

Teams provides chat-based workspace and collaboration opportunities. Teams also allows a variety of settings that control what users can or cannot do in chat or channel messages, such as send or delete messages, chat with organization users and external (federated) partners or vendor users, allow users to send email to a channel or allow third-party file storage, and so on.

As a Teams admin, you must be familiar with configuration settings including but not limited to chat messaging policies, external (federated) access, managing channels and teams, standard and private channel creation, email integration, configuration of external access for SharePoint and OneDrive for Business, and managing cloud file storage options for collaboration.

Tip You will encounter questions about how to control team creation and private channel creation, so you must be familiar with Office 365 Groups and their settings.

You might ask how to control chat and channel messages; the answer is to use messaging policy.

Messaging policy in Teams admin center (see Figure 8-5) controls chat and channel messages. There is also a channel setting for messages in Teams client. For example, if the team's owner wants to have an announcement channel in a team that only allows specific members to start a new post, you will set that here.

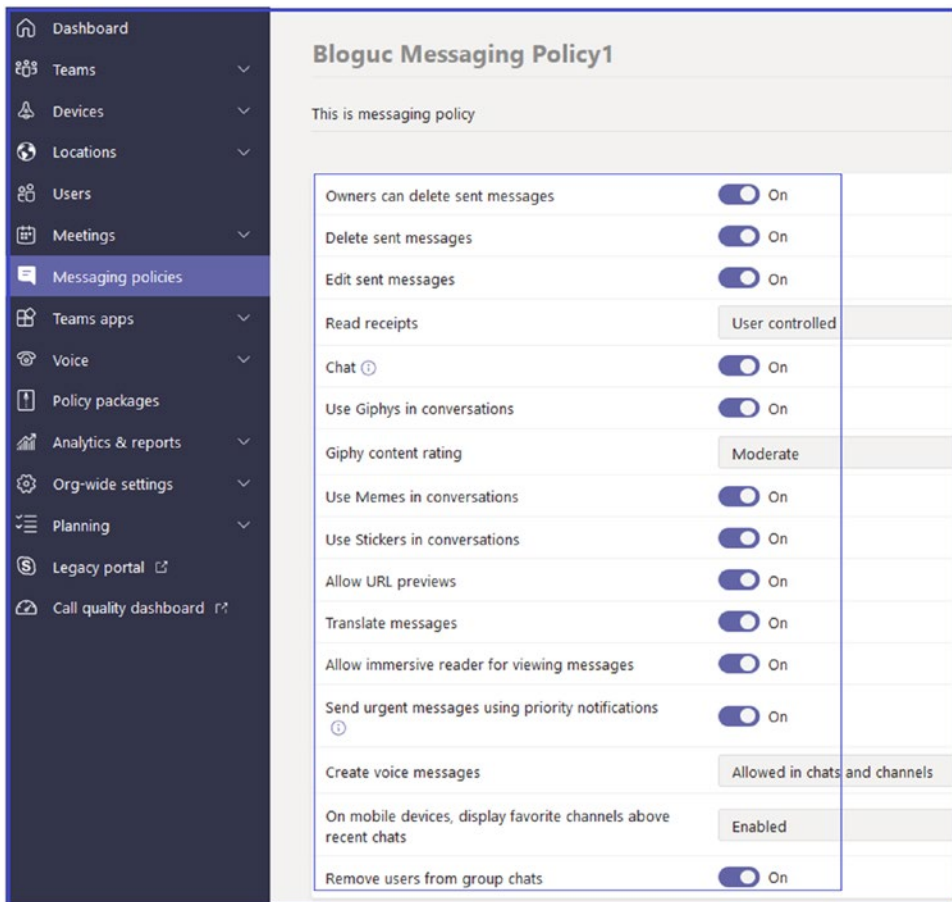


Figure 8-5. Messaging policies settings

To configure email integration, log in to Teams admin center, where you can set up email integration and cloud file storage, as shown in Figure 8-6.

Tip You might see a question on the exam asking for a list of file storage options. The answer is Citrix files, Dropbox, Box, and Google Drive.

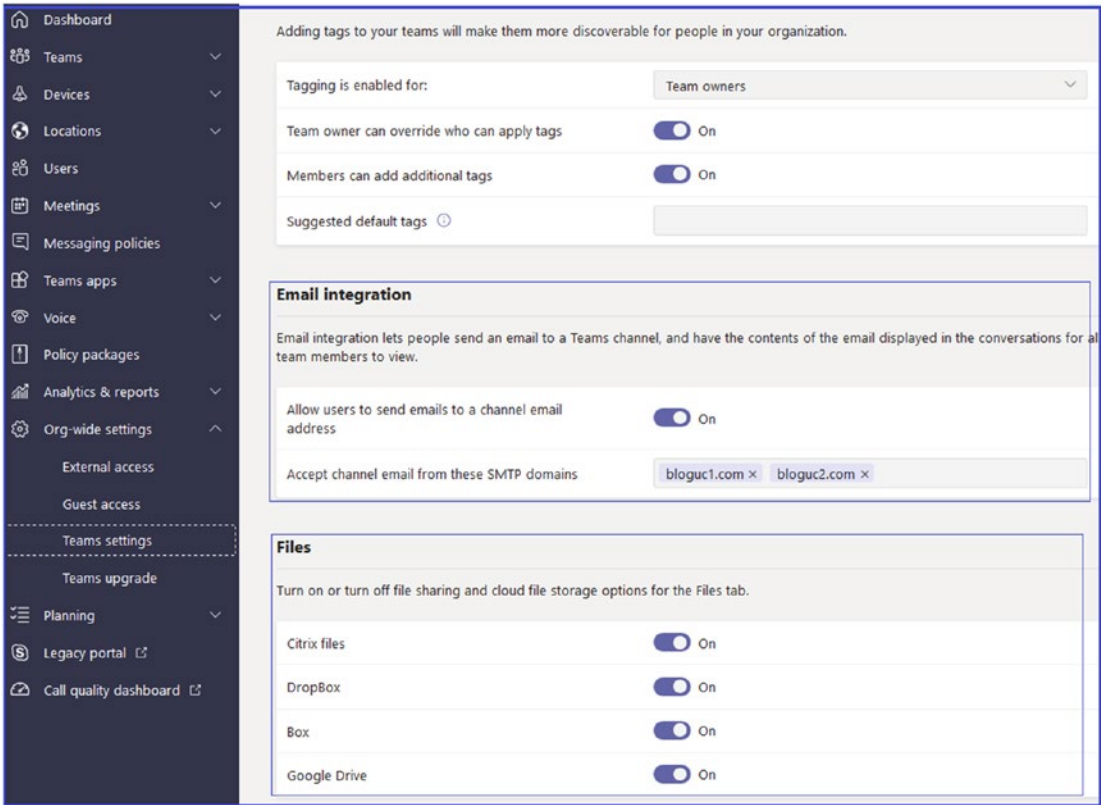


Figure 8-6. Teams email integration

Manage Meeting Experiences

You as a Teams admin can customize Teams meeting management settings under Teams Admin center ► Meetings. Select the appropriate option and set it accordingly. Meeting settings including allowing anonymous users to join the meeting, whether the user can request or give control, or what the user experience is while using a dial-in conference bridge. These are all features you can configure in a Teams meeting setting, based on your user and organization requirements [102].

Tip You might encounter questions about how to allow an anonymous user to join a Teams meeting. The answer is enabling the Anonymous Users Can Join A Meeting option in the meeting settings, as shown in Figure 8-7.

Meeting settings are set for meetings. You can customize, email invitations, and enable QoS by adding custom port ranges as per your organization's needs.

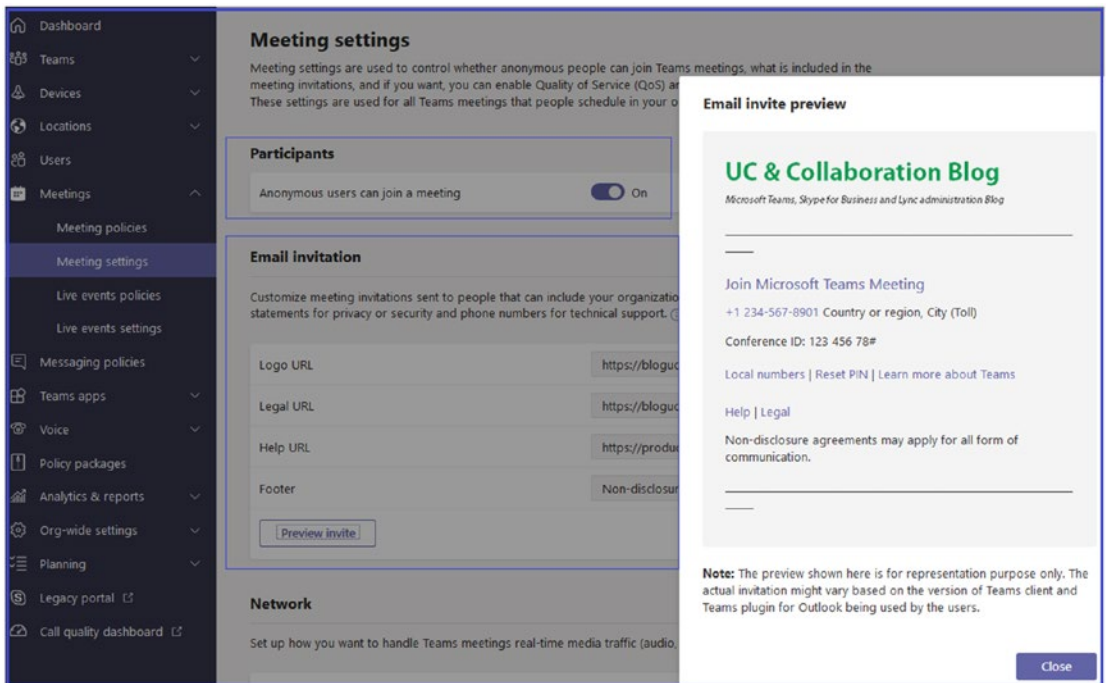


Figure 8-7. Teams meeting settings

Teams meeting policies do have several options you can turn on or off. Meeting policies settings are divided into four categories: General, Audio & Video, Content Sharing, and Participants & Guests, as shown in Figure 8-8.

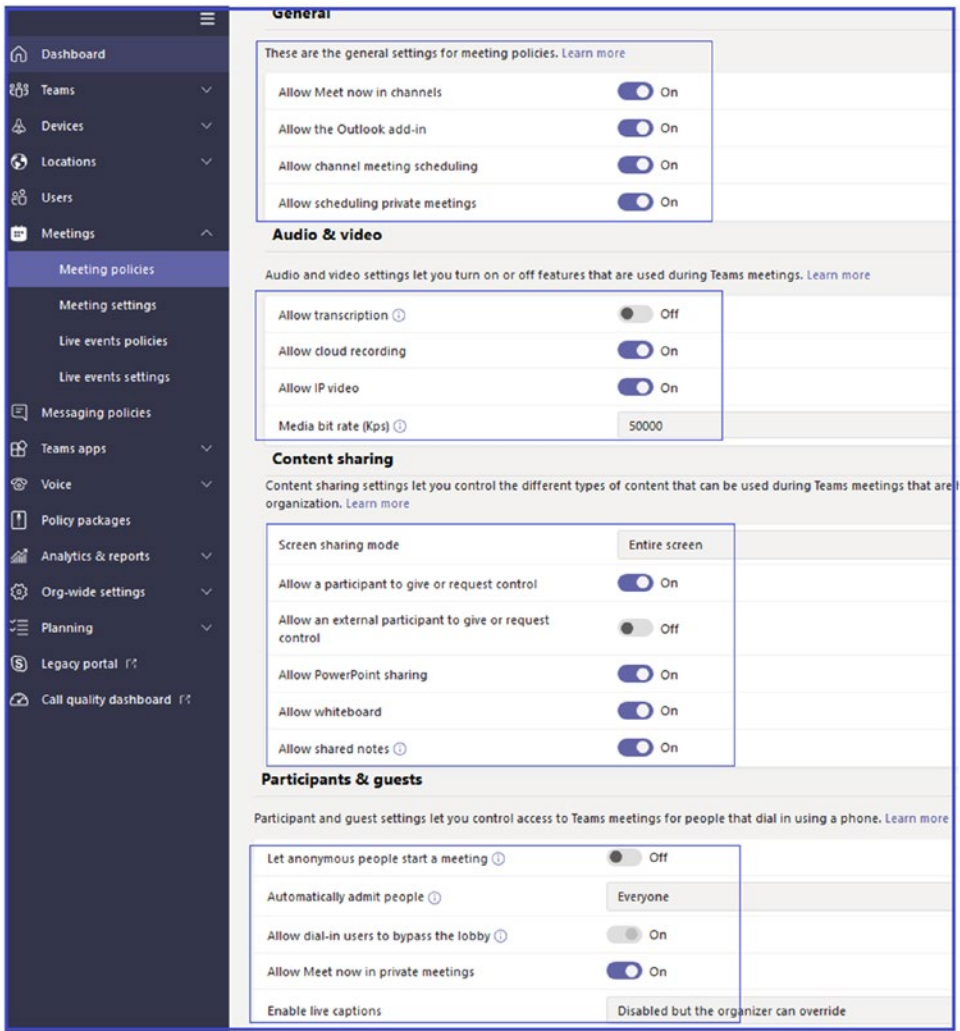


Figure 8-8. Meeting policies settings

Manage Phone Numbers

Teams requires a phone number when the user is enabled for enterprise voice to allow inbound and outbound phone calls. You, as an admin, need to understand different PSTN connectivity solutions based on the specific business requirements, like when to use Microsoft-provided Phone System Calling Plan and when to use Teams Phone System Direct Routing to leverage existing PSTN implementation including existing SBC. Based on the decision, there are different ways to get a phone number, and you can get the phone number from Microsoft or port it from an existing service provider to Microsoft [101].

There are different types of numbers, including numbers for users and numbers for services like a conference bridge, call queue, and auto attendant. You must be familiar with ordering phone numbers; managing service numbers; adding, changing, or removing an emergency address for your organization; assigning, changing, or removing a phone number for a user; and managing voice settings for users. You can refer to Chapter 4 for detailed information. Before the exam, you must be familiar with phone number orders and types of phones.

Tip You might be asked a question on phone number porting and different types of phone numbers.

Manage Phone System

You, as a Teams admin, need to be familiar with the Phone System Calling Plan and Phone System Direct Routing, so that you would be able to set up the policy. When the customer calls a hotline number, for example, how does that call get routed or handled? You must know how to configure a resource account for voice features such as call queue and auto attendant. There are various voice policies you can customize as well. You can change the display number (caller ID).

When the user reports a call drop issue, you need to check the Direct Routing dashboard to identify the potential issue. You must be familiar with different tasks such as managing resource accounts, creating and configuring call queues, creating and configuring auto attendants, managing call park policies, managing call policies, managing caller ID policies, and interpreting the Direct Routing health dashboard. To understand each task in detail, you can refer to Chapter 4.

Tip You might be asked a question about Phone System Calling Plan and Direct Routing, so be familiar with the setup and management process.

You might encounter a question on the Direct Routing health dashboard and its warnings. You need to interpret these warning to identify potential issues, so being familiar with Direct Routing setup and health dashboard is vital here.

Section 3: Manage Teams and App Policies

This third and final section of the Manage Microsoft Teams exam accounts for 20 to 25 percent of the exam questions. After enabling Teams for the organization, the next thing that you need to do as an admin is manage Teams effectively. Tasks include team creation, channel creation, integration of Teams with existing resources such as distribution groups, Office 365 Groups, SharePoint team site, and so on. For example, when a user reports an issue that teams don't appear in a search result, the teams' permission level comes into the picture. Setting up the right permission is essential.

Teams do have different types, such as public teams, private teams, and an org-wide team. Understanding the limitations of each type and knowing a way to convert existing teams to an org-wide team is also essential. You need to be familiar with the following task, as you might have a question on your exam about team management, membership management, and Teams app policy implementation.

- Manage a team.
- Manage membership in a team.
- Implement policies for Microsoft Teams apps.

Manage a Team

Managing a team includes creating a **team**, upgrading an **existing resource** to a team, managing **privacy levels** for a team, and managing **org-wide teams**.

Tip You might encounter questions with PowerShell commands for how to upgrade the distribution group to Office 365 Groups. The answer is to use the Upgrade-DistributionGroup PowerShell command; for example, Upgrade-DistributionGroup -DlIdentities IT@bloguc.com.

Manage Membership in a Team

After a team is created, managing membership in a team is an essential task. As a Teams admin, you must ensure the active users have access to Teams. Adding a new user and updating users who left the company are common activities that can be handling with Teams admin center or Windows PowerShell. Besides managing users manually, the

user list can be synced on the user attribute in Active Directory, such as a department. You must know how to automate membership management by creating a dynamic group for the user [102].

Tip You might encounter questions about how to automate membership management in a team. You can do that by creating a dynamic distribution group using this PowerShell command.

```
New-DynamicDistributionGroup -Name "Marketing Group"  
-IncludedRecipients "MailboxUsers,MailContacts"  
-ConditionalDepartment "Marketing","Sales"
```

Implement Policies for Microsoft Teams Apps

Implementing policies for Microsoft Teams apps and policy management is another critical topic. You must know where to block uploading custom apps and where to block third-party apps. If your organization only allows the developer to do side loading, then how would you configure the policy? The teams admin needs to know how to create a Teams setup policy and assign the policy to those supported teams.

Tip You might be asked questions on app permission policy creation and assignment. Refer to [Chapter 2](#) for detailed information.

Additional Resources for Exam Preparation

Microsoft presents a comprehensive collection of training options to empower technical professionals, help desk personnel, IT support persons, and even end users. Given that every person has a different learning style, it is better to select the methodology that works best for you.

If you are interested in learning more through digital (free online training) or instructor-led training (paid), there are partners that offer deep, technical training. Use the following resources for further learning.

- *Course details:* <https://docs.microsoft.com/en-us/learn/certifications/courses/ms-700t00>
- *Instructor-led training through partners:* <https://docs.microsoft.com/en-us/learn/certifications/exams/ms-700?tab=tab-instructor-led>
- *Free training:* Manage team collaboration with Microsoft Teams: <https://docs.microsoft.com/en-us/learn/paths/m365-manage-team-collaboration/>

Summary

Microsoft Teams focuses on effective and efficient collaboration and communication in an enterprise environment. You must understand the complete administration process, which includes access issues, management, and call quality problems. Before taking an exam, you, as an admin, must be able to plan, deploy, adapt, communicate, and manage all Teams features. You will be responsible for upgrading user workload from Skype for Business to Microsoft Teams, and must be acquainted with telephony integration and Teams Phone System Direct Routing using SBC and Teams Phone System Calling Plan and Teams Audio (dial-in) Conferencing.

Glossary

ACLs: access control lists
ADDS: Active Directory Domain Service
ADFS: Active Directory Federation Services
API: application programming interface
ASCII: American Standard Code for Information Interchange
AV MCU: audio video multi-control unit
Azure AD: Azure Active Directory
B2B: business-to-business
CA: conditional access
CDN: content delivery network
DID: Direct Inward Dialing
DNS: Domain Name System
DR: Direct Routing
DSCP: Differentiated Services Code Point
E.164: Phone number format (globally accepted format)
E911: Enhanced 911
eCDN: Enterprise Content Delivery Network
ELIN: Emergency Location Identification Number
EML format: EML files can contain plain ASCII text for the headers and the main message body as well as hyperlinks and attachments
GPO: Group Policy object
GUI: graphical user interface
HD: High Definition
ICE: Interactive Connectivity Establishment
IDS: intrusion detection
IPS: intrusion prevention system
KBPS: kilobits per second
MA: modern authentication

GLOSSARY

MBPS: megabytes per second
MDM: Mobile Device Management
MFA: multifactor authentication
NAT: Network Address Translation
OS: operating system
PAT: Port Address Translation
PBX: private branch exchange
PIN: personal identification number
POC: proof of concept
PSAP: Public Safety Answering Point
PSTN: public switched telephone network
QoS: Quality of Service
RBAC: role-based access control
RegEX: regular expression
RNL: reverse number lookup
SAML: Security Assertion Markup Language
SBC: session border controller
SDN: Software Defined Networking
SFA: single-factor authentication
SLA: service-level agreement
SMTP: Simple Mail Transfer Protocol
SSO: single sign-on
STUN: Session Traversal Utilities for NAT
TCP: Transmission Control Protocol
TDR: Teams Direct Routing
TURN: Traversal Using Relay NAT
UDP: User Datagram Protocol
UI: user interface
UPN: User Principal Name
URL: Uniform Resource Locator
VPN: virtual private network
WMM: Wi-Fi Multimedia

References

- [1] Microsoft Teams definition. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/teams-overview>
- [2] Definition word. Retrieved from <https://www.lexico.com/en/definition/architecture>
- [3] Microsoft Ignite, Manage Microsoft Teams. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/81821>
- [4] Microsoft Teams logical architecture. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/teams-architecture-solutions-posters>
- [4a] Microsoft Teams architecture details. Retrieved from <https://bloguc.com/microsoft-teams-different-components-and-logical-architecture/>
- [5] What's new in Microsoft Teams. Retrieved November 5, 2019, from support.office.com.
- [6] Microsoft Teams: 7 things you need to know. Retrieved from <https://www.cnet.com/news/microsoft-teams-7-things-you-need-to-know/>
- [7] Microsoft Teams review. Retrieved November 6, 2019. <https://docs.microsoft.com/en-us/microsoftteams/teams-channels-overview>
- [7a] Microsoft Teams architecture update. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/83471>
- [8] What is Microsoft Teams definition. Retrieved from https://en.wikipedia.org/wiki/Microsoft_Teams
- [9] Microsoft Teams definition. Retrieved from <https://docs.microsoft.com/en-us/learn/modules/m365-teams-collab-prepare-deployment/explore-user-experience>
- [10] Teams Custom Tab. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/built-in-custom-tabs>
- [11] Microsoft Teams licensing. Retrieved from <https://docs.microsoft.com/microsoftteams/office-365-licensing>
- [12] Teams governance. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/plan-teams-governance>

REFERENCES

- [13] Plan for Teams lifecycle management information. Retrieved from <https://docs.microsoft.com/microsoftteams/plan-teams-lifecycle>
- [14] Network planning and preparation information. Retrieved from <https://docs.microsoft.com/microsoftteams/upgrade-prepare-environment-prepare-network>
- [14a] Network planning and bandwidth requirement. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/prepare-network>
- [14b] VPN split tunnel implementation information. Retrieved from <https://bloguc.com/implement-vpn-split-tunnel-for-microsoft-teams-media-traffic/>
- [15] Teams client hardware requirement. Retrieved from <https://docs.microsoft.com/microsoftteams/hardware-requirements-for-the-teams-app>
- [16] Get Teams Mac client information. Retrieved from <https://docs.microsoft.com/microsoftteams/get-clients#mac>
- [17] Teams support browser. Retrieved from <https://docs.microsoft.com/microsoftteams/limits-specifications-teams#browsers>
- [18] Teams org-wide team creation. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/create-an-org-wide-team>
- [19] Assign team owner and member in Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/assign-roles-permissions>
- [19a] Team owner, member and guest permission. Retrieved from <https://support.office.com/en-us/article/team-owner-member-and-guest-capabilities-in-teams-d03fdf5b-1a6e-48e4-8e07-b13e1350ec7b#ID0EAABAAA=Desktop>
- [20] Office 365 group and Microsoft Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/office-365-groups>
- [21a] Authorize guest access. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-dependencies>
- [21b] Microsoft Teams guest access: How it works and images. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/85261>
- [22] Manage external access in Microsoft Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/manage-external-access>
- [22a] Security and compliance in Microsoft Teams information. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/83470>
- [23] Dynamic membership for Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/dynamic-memberships>
- [23a] Data loss prevention policy for Teams. Retrieved from <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams>

- [24] Manage messaging policy in Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/messaging-policies-in-teams>
- [24a] Manage information barrier. Retrieved from <https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers>
- [25] Apps, Bot and connectors in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/deploy-apps-microsoft-teams-landing-page>
- [26] Admin settings for apps. Retrieved from <https://docs.microsoft.com/microsoftteams/admin-settings>
- [27] Use built-in and custom apps in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/built-in-custom-tabs>
- [28] Add bots for personal chat, group chat and channels in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/add-bots>
- [28a] Teams private channel information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/private-channels>
- [29] Use Office 365 and custom connectors in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/office-365-custom-connectors>
- [30] Teams meeting clients. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/tutorial-meetings-in-teams?tutorial-step=3>
- [31] Meeting and conferencing in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/deploy-meetings-microsoft-teams-landing-page>
- [32] Meetings in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/tutorial-meetings-in-teams?tutorial-step=1>
- [33] Manage meeting policy in Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/meeting-policies-in-teams>
- [34] Teams cloud meeting recording. Retrieved from <https://docs.microsoft.com/microsoftteams/cloud-recording>
- [35] Audio Conferencing in Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/deploy-audio-conferencing-teams-landing-page>
- [36] Audio Conferencing common questions. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/audio-conferencing-common-questions>
- [37] Country and region availability for Audio Conferencing and Calling Plan. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/country-and-region-availability-for-audio-conferencing-and-calling-plans/country-and-region-availability-for-audio-conferencing-and-calling-plans>

REFERENCES

- [38] What are Microsoft Teams live events? Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-live-events/what-are-teams-live-events>
- [39] Plan for live event in Microsoft Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-live-events/plan-for-teams-live-events>
- [40] Call Analytics and Call Quality Dashboard. Retrieved from <https://docs.microsoft.com/microsoftteams/difference-between-call-analytics-and-call-quality-dashboard>
- [41] Welcome to Microsoft Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-overview>
- [42] Getting started with your Microsoft Teams upgrade. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-start-here>
- [43] Upgrade from Skype for Business to Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-to-teams-on-prem-overview>
- [44] Teams upgrade planning workshop. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-workshops-landing-page>
- [45] Teams client experience and conformance to coexistence mode. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-client-experience-and-conformance-to-coexistence-modes>
- [46] Understand Microsoft Teams and Skype for Business coexistence and interoperability. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-and-skypeforbusiness-coexistence-and-interoperability>
- [47] Plan hybrid connectivity between Skype for Business server and Office 365. Retrieved from <https://docs.microsoft.com/SkypeForBusiness/hybrid/plan-hybrid-connectivity?toc=/SkypeForBusiness/sfbhybridtoc/toc.json>
- [48] Prepare your environment for Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-prepare-environment-prepare-service>
- [49] Evaluate your environment before teams upgrade. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-plan-journey-evaluate-environment>
- [50] Prepare environment for Teams upgrade. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-prepare-environment>
- [51] Prepare IT staff for Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-prepare-it-pros>
- [52] Prerequisites and environment dependencies for Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-plan-journey-prerequisites>

- [53] Prepare Office 365 for Teams. Retrieved from <https://docs.microsoft.com/microsoftteams/office-365-groups>
- [54] Configure Teams core capabilities details. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/deploy-chat-teams-channels-microsoft-teams-landing-page>
- [55] Configure networking. Retrieved from <https://docs.microsoft.com/microsoftteams/upgrade-prepare-environment-prepare-network>
- [56] Configure cloud voice workload in Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/cloud-voice-landing-page>
- [57] Configure Direct Routing in Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/direct-routing-landing-page>
- [57a] Managing Microsoft Teams Direct routing information. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/83183>
- [58] Prepare your service for upgrading to Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-prepare-environment-prepare-service>
- [59] Teams client experience and conformance to coexistence mode. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/teams-client-experience-and-conformance-to-coexistence-modes>
- [60] Setting your coexistence and upgrade settings. Retrieved from <https://aka.ms/SkypeToTeams-SetCoexistence>
- [61] Upgrade from Skype for Business online to TeamsOnly mode. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-to-teams-execute-skypeforbusinessonline>
- [62] Upgrade from Skype for Business on-premise to Teams. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/upgrade-to-teams-execute-skypeforbusinesshybridonprem>
- [63] Move users between on-premise and the cloud. Retrieved from <https://docs.microsoft.com/skypeforbusiness/hybrid/move-users-between-on-premises-and-cloud>
- [64] TeamsUpgrade policy managing and migrating and coexistence. Retrieved from <https://docs.microsoft.com/MicrosoftTeams/migration-interop-guidance-for-teams-with-skype#teamsupgradepolicy-managing-migration-and-co-existence>
- [65] Configure Azure AD connect for Teams and Skype for Business. Retrieved from <https://docs.microsoft.com/SkypeForBusiness/hybrid/configure-azure-ad-connect>

REFERENCES

- [66] Effectively organize broadcasts using Microsoft live events. <https://bloguc.com/effectively-organize-broadcasts-using-microsoft-live-events/>
- [67] How does Microsoft Teams live events works? Retrieved from <https://bloguc.com/how-does-microsoft-teams-live-event-works/>
- [68] Microsoft Teams live event architecture. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/83196>
- [68a] Microsoft Stream architecture. Retrieved from <https://bloguc.com/microsoft-stream-architecture-details/>
- [69] Microsoft Stream architecture and administration information. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/81526>
- [69a] Microsoft Stream group and their structure. Retrieved from <https://docs.microsoft.com/en-us/stream/groups-channels-organization>
- [70] What is the Public Switched Telephone Network? Retrieved from https://en.wikipedia.org/wiki/Public_switched_telephone_network
- [71] Teams Phone System. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/what-is-phone-system-in-office-365>
- [72] Managing Microsoft Teams (MS 700) exam preparation and planning. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/85219>
- [73] Manage team collaboration with Microsoft Teams. Retrieved from <https://docs.microsoft.com/en-us/learn/paths/m365-manage-team-collaboration/>
- [74] Microsoft Teams sign-in procedure. Retrieved from <https://docs.microsoft.com/en-us/MicrosoftTeams/sign-in-teams>
- [75] What is auto attendant and how directory search work in AA. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/what-are-phone-system-auto-attendants>
- [76] Microsoft Teams apps deployment and management. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/msi-deployment>
- [76a] Microsoft Teams client hardware and software requirements. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/itadmin-readiness>
- [77] Microsoft Teams Room. Retrieved from <https://docs.microsoft.com/en-us/MicrosoftTeams/rooms/with-office-365>
- [78] Manage emergency addresses in Teams information. Retrieved from <https://docs.microsoft.com/en-us/MicrosoftTeams/what-are-emergency-locations-addresses-and-call-routing>

- [79] Manage Teams Emergency calling policy. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/manage-emergency-calling-policies>
- [80] Manage Teams emergency call routing policies. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/manage-emergency-call-routing-policies>
- [81] Create and manage custom dial-plan details. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/create-and-manage-dial-plans>
- [82] Create and manage Teams calling policy information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/teams-calling-policy>
- [83] Access and manage Teams analytics and report information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/teams-analytics-and-reports/teams-reporting-reference>
- [84] Teams upgrade policy using PowerShell information. Retrieved from <https://docs.microsoft.com/en-us/powershell/module/skype/grant-csteamsupgradepolicy?view=skype-ps>
- [85] Microsoft 365 Admin center and report. Retrieved from <https://docs.microsoft.com/en-us/office365/admin/activity-reports/activity-reports?view=o365-worldwide>
- [86] Microsoft Teams Direct routing solutions. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan>
- [87] Teams Audio Conferencing and Communications Credits information. Retrieved from <https://bloguc.com/how-microsoft-teams-audio-conferencing-dial-out-and-call-me-at-call-charges-estimates/>
- [88] Setup Communications Credits for Teams audio conferencing information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/set-up-communications-credits-for-your-organization>
- [89] Teams calling plan and how to setup information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/set-up-calling-plans>
- [90] Teams Direct Routing PSTN gateway command parameter information. Retrieved from <https://docs.microsoft.com/en-us/powershell/module/skype/new-sonlinepstngateway>
- [91] Create and manage call queue and resource account information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/create-a-phone-system-call-queue>

REFERENCES

- [92] Understand, create and manage emergency calling service and policy information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/configure-dynamic-emergency-calling>
- [93] Create manage emergency policy information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/manage-emergency-calling-policies>
- [94] Create and manage Voice routing policy. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-voice-routing>
- [95] Manage Office 365 group lifecycle information. Retrieved from <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle>
- [96] Office 365 restoration. Retrieved from <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted>
- [97] SfB to Teams migration path and user migration. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/83478>
- [98] Teams login issues with known error code. Retrieved from <https://support.office.com/en-us/article/why-am-i-having-trouble-signing-in-to-microsoft-teams-a02f683b-61a3-4008-9447-ee60c5593b0f>
- [99] Teams management details and troubleshooting information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/monitor-call-quality-qos>
- [99a] Teams QoS implementation information. Retrieved from <https://bloguc.com/implement-quality-of-service-qos-for-microsoft-teams/>
- [100] Teams service health information. Retrieved from <https://docs.microsoft.com/en-us/microsoftteams/service-health>
- [101] Managing Microsoft Teams exam. Retrieved from <https://myignite.techcommunity.microsoft.com/sessions/85219>
- [102] Dynamic distribution group PowerShell command. Retrieved from <https://docs.microsoft.com/en-us/powershell/module/exchange/users-and-groups/new-dynamicdistributiongroup?view=exchange-ps>
- [103] Microsoft Teams meeting Outlook add-ins. Retrieved from <https://bloguc.com/how-do-teams-meeting-add-ins-working-in-outlook/>
- [104] Microsoft Teams various feature maximum limitation and expiration period information. Retrieved from <https://bloguc.com/various-limit-and-expiration-period-applied-in-microsoft-teams-capabilities/>

Index

A

- Access control lists (ACLs), [248](#)
- Active Directory Domain Service (ADDS), [38](#)
- Active Directory Federation Services [ADFS], [16](#)
- Ad-hoc meeting, [30](#)
- Advanced Encryption Standard (AES), [19](#)
- Advisor for Teams, [204](#), [205](#)
 - assessment, [207](#)
 - deploying workloads, [205](#)
 - use, [205](#)
- Analytics & Reports tab, [166](#), [167](#)
- Architecture, Office 365, [3](#)
- Attendant routing, [309](#)
- Audio and Video Call Quality Issue
 - troubleshooting
 - call analytics, [448–450](#)
 - CQD, [450](#), [451](#)
 - devices, [444](#), [446](#)
 - issues, [442](#), [443](#)
 - network, [443](#)
 - one-one call, [446](#), [447](#)
 - VOIP, [442](#)
- Audio and video calls and meetings (VoIP), [442](#)
- Audio conferencing
 - adding dedicated conference bridge number, [284](#)
 - Communications Credits (*see* Communications Credits)
 - configuring/managing conference
 - bridge settings, [285](#), [286](#)
 - default conference bridge
 - number, [284](#), [285](#)
 - license, [282](#)
 - Network Testing Companion tool, [282](#)
 - requirements, [282](#), [283](#)
 - settings, [282](#)
 - Teams dial-in conferencing, [282](#)
 - Teams meeting policies, [292](#)
- Audio streams, [218](#)
- Auto attendants
 - adding, [314](#)
 - assigning phone work, [320](#)
 - call routing options, [316](#)
 - features, [312](#)
 - fine people settings, [319](#)
 - greeting message, [315](#)
 - holiday call settings, [318](#)
 - managing, [320](#)
 - maximum directory size, [321](#)
 - menu system, [312](#), [322](#)
 - prerequisites, [313](#)
 - resource account, [313](#), [319](#)
 - searching for users, [320](#), [321](#)
 - set business hours, [317](#)
- Auto-Recharge option, [289](#)
- Azure active directory center, [218](#)

INDEX

Azure active directory center (*cont.*)
access, [219, 220](#)
admin center, [220](#)

B

Bloguc Organization, [180](#)
Business Online module, [226, 227](#)

C

Call analytics, [281](#)
Caller ID policies, [161, 163](#)
 custom, [162](#)
 PowerShell module, [163, 164](#)
Calling Plan, [330, 339](#)
 assigning users, [304, 305](#)
 options, [301](#)
 PSTN, [301](#)
 purchasing, [304](#)
 set up, [302, 303](#)
Calling policies, [158](#)
 creation, [159](#)
 custom, [158](#)
 settings, [160, 161](#)
 user, [159, 160](#)
Call park policy, [155](#)
 assign, [157](#)
 creation, [156](#)
 PowerShell, [157](#)
 users, [157](#)
Call Quality Dashboard (CQD), [214, 474](#)
 dashboards, [215, 216](#)
 endpoint, [215](#)
 list, [216](#)
 use, [214](#)
Call queues
 agent selection, [308](#)
 auto attendant, [305](#)

 creation, [306, 307](#)
 distribution method, [309](#)
 features, [305](#)
 greeting/music selection, [308](#)
 manage, [311, 312](#)
 overflow handling, [310](#)
 redirect settings, [310](#)
 resource account, [305, 307](#)
 time out handling, [311](#)
Call Quality Dashboard (CQD), [450](#)
Channel meetings, [269](#)
Channels, [13, 15](#)
Client-side troubleshooting
 audience size maximum limit, [439](#)
 channel limitations, [441](#)
 channel names, [442](#)
 chat limitations, [440, 441](#)
 expiration limits, [438](#)
 maximum limit, [439, 440](#)
 meeting, number of people, [439](#)
 PowerPoint presentations, [439](#)
 updates, [436, 437](#)
Cloud Connector Edition (CCE), [406](#)
Cloud Identity model, [16](#)
Communications Credits
 individual user's conference bridge
 number, [291, 292](#)
 plans/pricing, [288](#)
 procedure, [288–290](#)
 setting up, [286–288](#)
 tenant's PSTN usage, [290](#)
Conditional access policy
 access controls, [352](#)
 assignment, [350](#)
 Cloud app, [350](#)
 creation, [353](#)
 device platforms, [351](#)
 procedure, [349](#)

- settings, [352](#)
- sign-in risk level, [351](#)
- Configure Multifactor Authentication
 - kinds, [41](#)
 - working, [41](#), [42](#)
- Content Delivery Network (CDN), [21](#)
- Content sharing, [278](#)
- Custom dial plan, [140](#)

D

- Data loss prevention (DLP), [341](#), [471](#)
 - admin, [354](#)
 - creation, [356–358](#)
 - locations, [359](#)
 - name/description, [358](#)
 - policies, [354–356](#)
 - review, [362](#)
 - sensitive information, [360](#)
 - settings, [360](#)
 - testing, [361](#)
- Devices
 - assign, [86](#), [87](#)
 - configuration profiles, [83](#), [84](#)
 - management options, [88](#)
 - network settings, [86](#)
 - phone, [82](#), [83](#)
 - phone configuration, [84](#)
 - phone inventory, [87](#)
 - settings, [85](#)
- Dial plans, [139](#)
- Differentiated Services Code Point (DSCP)
 - markings, [246](#)
- Direct Inward Dial (DID), [407](#)
- Direct Routing, [146](#), [147](#), [339](#)
 - Business Online PowerShell, [151](#), [152](#)
 - configuration, [150](#)
 - dashboard, [154](#)

- managing teams, [154](#)
- PSTN gateway, [152–154](#)
- SBC view, [155](#)
- scenarios, [147](#), [148](#)
- Direct Routing solution, [148–150](#)
- Dynamic emergency calling
 - direct routing, [331](#)
 - emergency routing, [333](#)
 - network settings, [329](#), [330](#)
 - network topology, [328](#)
 - notification group, [334](#)
 - preparation work, [328](#), [329](#)
 - procedure, [332](#)
 - PSTN phone number, [332](#)

E

- Email integration, [189–191](#)
- Emergency addresses, [92](#)
- Emergency calling service
 - configuration, [323](#), [324](#)
 - direct routing, [326](#)
 - E911, [322](#)
 - Phone System Calling
 - Plan, [324–326](#)
 - physical/street address, [323](#)
 - PSAP, [322](#)
 - TeamsEmergencyCallRoutingPolicy,
 - [327](#), [328](#)
 - validation, [324](#)
- Enhanced 911 (E911), [322](#)
- Enterprise Content Delivery Network (eCDN), [21](#)
- Exchange online, [10](#), [89](#)
- External access, [175](#), [176](#)
 - federation, [177](#)
 - guest access, [179–182](#)
 - specific domain, [178](#), [179](#)

F

- Failover response codes, 298
- Federated Identity model, 16
- File storage options, 191, 192
- Force switch, 298
- Fully Qualified Domain Name (FQDN), 297

G

- Gesturing, 232
- Global Address List (GAL), 381
- Governance and life cycle management, 341
 - business-critical information, 347
 - DLP (*see* Data loss prevention (DLP))
 - eDiscovery workflows, 363
 - identity and access management (*see* Identity and access management)
 - retention (*see* Retention policies)
 - security, 348
 - single platform, 347
- Government Community Cloud (GCC), 20
- Grant-CsTeamsUpgradePolicy command, 404
- Graphical user interface (GUI), 76
- Group expiration policy
 - Bloguc organization, 376
 - configuration, 377
 - directory system, 376
 - email notification, 377, 380
 - retention policy, 379
 - settings page, 378, 379
- Group Policy object (GPO), 91
- Group Policy objects (GPOs), 246
- Guest access, 179
 - calling/meetings, 183
 - message settings, 185, 186

H

- Human resources (HR), 370

I, J, K

- Identity and access management
 - conditional access (*see* Conditional access policy)
 - risk assessment, 348
 - user experience, 353
- Information barrier (IB)
 - between groups, 371
 - ethical wall, 370
 - logical boundaries, 370
 - policies, 371
 - prerequisites, 372, 373
 - set up, 371
- Intelligent communications cloud
 - next-generation services, 4
 - Skype next-generation service, 4
 - stack, 5
 - VoIP, 4, 5
- Internal users, 31
- Intrusion detection system (IDS), 235
- Intrusion prevention system (IPS), 235
- Islands mode
 - features, 396–398
 - overlapping capabilities, 395
 - Skype for Business, 395, 396
 - online, 398, 399
 - on-premises, 399, 400
 - Upgrade coexistence mode, 401–403

L

- Latency-sensitive application, 246
- Legacy portal, 213, 214
- Live event

- attendee, 23
 - external app/device, 24, 25
 - high-level architecture, 21
 - media flow, 22
 - minimum knowledge, 25–27
 - one-to-many communications, 20
 - organizer, 23
 - producer view, 23, 28
 - production, teams, 24
 - tenant admin, 23
 - Live events, 67
 - configuration/management, 69
 - new policy, 73
 - policies, 71, 72
 - PowerShell, 71
 - record, 74
 - settings, 70
 - Teams admin center, 69, 72
 - third-party distribution, 70
 - Microsoft Stream, 67
 - overview, 68, 69
 - Location-Based Routing (LBR), 299
 - Locations Tab, 91
 - emergency addresses, 92–95
 - emergency location, 95
 - reporting labels, 91
 - upload reporting labels, 91, 92
- M**
- Managing identity, 219
 - Managing internal risk
 - organizations face, 370
 - sensitive information, 370
 - Managing Microsoft Teams
 - (MMT), 463
 - direct routing, 464
 - exam
 - business environment, upgrade
 - skype, 466, 467
 - chat/calling/meetings, 476
 - chat/collaboration
 - experiences, 476–478
 - configure/manage guest access, 470
 - deploy/manage microsoft teams
 - endpoints, 472, 473
 - governance/life cycle
 - management, 468–470
 - manage meeting experiences,
 - 478, 479
 - manage membership, 482
 - manage security/compliance, 471
 - monitor/analyze service
 - usage, 474, 475
 - phone system, 480, 481
 - plan/configure environment, 465
 - plan/configuring network settings,
 - 467, 468
 - policies, 483
 - resources, 483
 - teams/app policies, 482
 - exam structure, 464
 - Managing internal risk
 - IB (*see* Information barrier (IB))
 - Media bypass parameter, 300
 - Meeting Migration Service
 - (MMS), 416, 417
 - Meeting policies, 99
 - application, 100
 - assignment, 105
 - audio/video, 102, 278, 279
 - content sharing, 103
 - creation, 100
 - email invitation, 107, 108
 - feature, 279
 - general settings, 277

INDEX

Meeting policies (*cont.*)

- guest features, 104
- management, 107
- network, 108
- participant/grant settings, 280
- participants, 107
- sections, 276
- setting, 101
- Users tab, 106

Meetings tab, 99

Messaging policy, 109

- creation, 110, 111
- modify/delete, 113
- PowerShell, 114
- user assign, 112

Microsoft, attendee, types, 31

Microsoft 365 admin center, 220

- access, 221
- compliance center, 223–225
- dashboard, 221, 222
- identities, 224
- PowerShell, 225

Microsoft Office 365 services

- application, 6
- components, 5
- features, 5

Microsoft Stream, 74

- access, 75
- architecture, 17–19
- channels, 75, 76
- data residing, 20
- group view, 75
- live events, 17
- Teams video recording, 17

Microsoft Teams

- administrative roles, 428
- administrator-based troubleshooting, 425

approach, 432, 433

architecture (*see* Architecture)

- capabilities, 35
- capabilities/data storage locations, 7, 8
- channels, 13, 15
- client logs, 433–435
- cloud platform, 1
- connectivity issues, 442
- definition, 2, 425
- deployment, 231, 262
- features, 231
- files, 17
- identity models, 15, 16
- licensing requirement, 33–35
- live event (*see* Live event)
- logical architecture, 8–10
- MA, 429
- managed/unmanaged network, 247
- meetings, 29, 30
- network traces, 427
- Office 365 services, 10, 11, 455
- PSTN (*see* Phone System (PSTN) call troubleshooting)
- RNL, 426
- sign-in issues/error codes, 429–431
- tabs, 16
- team, 11, 12
- third-party apps integration, 35
- tools
 - network assessment, 458–460
 - service health, 455–457
 - SIP tester, 460
- troubleshooting (*see* Client-side troubleshooting)
- unified conversation platform, 1
- URL dependencies, 426
- voice/ video call capabilities, 28
- VPN, 231

- Microsoft Teams Administrator, 463
 - Microsoft Teams conferences, 264
 - Microsoft Teams media traffic
 - client source port ranges, 247
 - DSCP marking, network layer, 248
 - Qos (*see* Quality of Service (QoS) policies)
 - Microsoft Teams PowerShell, 228
 - Migration path and coexistence modes
 - list, 390
 - planned deployment path, 394, 395
 - planning/implementation, 391, 392
 - POC, 391
 - Skype for business, 390–393
 - Teams side-by-side (Islands) mode (*see* Islands mode)
 - user readiness, 391
 - Modern authentication (MA), 429
 - Move-CsUser PowerShell, 404
 - msRTC SIP attribute, 398, 404
 - Multicontrol unit (MCU), 260
 - Multifactor authentication (MFA), 39
- N**
- Naming policy
 - add/remove, 384
 - Azure AD PowerShell module, 383
 - creating/managing, 381, 383
 - custom blocked words, 384, 385
 - prefixes/suffixes, 381
 - Native interoperability experience
 - desktop sharing, 415
 - one-to-one chat and call, 414
 - Teams meeting, 416
 - Network Address Translation (NAT), 235
 - Network assessment
 - optimal traffic flows, 232
 - Teams deployment, 233–235
 - teams media traffic, 232
 - teams signaling traffic, 232
 - traffic types, 232
 - WAN, 232
 - Network Bandwidth
 - accepted limits, 236
 - latency/packet-loss issues, 236
 - network quality, 236
 - Teams call scenarios, 237
 - Network planner, 207, 208, 273
 - assigning, 209
 - bandwidth requirements, 237
 - building, 209
 - determine/organize, 238, 239
 - report, 212, 213
 - site/subnet, 240, 241
 - subnet, 211
 - tool, 237
 - Network testing companion tool
 - audio quality test, 244
 - connectivity, 244
 - installation, 242
 - IPs/ports, 245
 - Microsoft Transport Relay
 - network, 243
 - optimal call quality, 241
 - planning phase, 241
 - prerequisites, 241
 - result analyzer, 245
 - Network topology, 95, 96
 - IP address, 97, 98
 - subnet, 97
 - Normalization rule, 142
 - Normalization type
 - selection, 143
 - Notification and feeds
 - settings, 187, 189

O

- Office 365 Groups
 - classify content, [373](#)
 - configuring
 - classifications, [375, 376](#)
 - enabling, [374, 375](#)
 - expiration policy (*see* Group expiration policy)
 - functionality, [373](#)
 - naming policy (*see* Naming policy)
- OneDrive, [9](#)
- Online PSTN gateway
 - Enabled, [297](#)
 - ExcludedCodecs, [298](#)
 - FailoverResponseCodes, [298](#)
 - FailoverTimeSeconds, [298](#)
 - Force, [298](#)
 - ForwardCallHistory, [297](#)
 - ForwardPai, [299](#)
 - ForwardPAI, [297](#)
 - Fqdn, [297](#)
 - GatewaySiteLbrEnabled, [299](#)
 - GenerateRingingWhileLocating User, [299](#)
 - Identity, [296](#)
 - InboundPSTNNumberTranslation Rules, [296](#)
 - InboundTeamsNumberTranslation Rules, [296](#)
 - MaxConcurrentSessions, [299](#)
 - MediaBypass, [300](#)
 - OutboundPSTNNumberTranslation Rules, [296](#)
 - OutboundTeamsNumberTranslation Rules, [296](#)
 - SBC configuration, [295](#)
 - SendSipOptions, [300](#)

- SipSignalingPort, [297](#)
- Teams, [300](#)
- On-Premises enterprise voice
 - to Teams
 - coexistence mode, [407](#)
 - DID, [407](#)
 - feature functions, [409](#)
 - PowerShell script, [409–411](#)
 - readiness plan, [409](#)
 - upgrading, [408](#)
 - user provisioning, [407](#)
 - voice routing policy, [407](#)
- Organization tab, [192, 193](#)
 - coexistence modes, [199](#)
 - devices, [193, 194](#)
 - individual user, [201, 202](#)
 - name search, [194, 195](#)
 - setting Teams, [199, 200](#)
 - upgrade, [196–198, 201, 203](#)
 - Windows PowerShell, [203, 204](#)
- Organizing Teams meetings
 - calendar daily/weekly view, [265](#)
 - chat with participants option, [267](#)
 - controls, [269](#)
 - joining, [268](#)
 - setting up, [266](#)

P

- P-Asserted-Identity (PAI), [299, 337](#)
- Personally Identifiable Information (PII), [358](#)
- Phone/service number
 - order, [336](#)
 - procedure, [335](#)
- Phone System Planning
 - audio/video calls, [294](#)
 - direct routing, [294, 295](#)

Online PSTN gateway (*see* Online PSTN gateway)
 permits users, 293

Phone System (PSTN) call
 troubleshooting
 call failures, 453, 454
 connect voicemail, 454
 Outlook connectivity, 454
 phone dial-pad, 453
 restoring deleted channel, 455
 teams client call features,
 451, 452

Policy assignment, 164

Policy-based QoS, 249

Policy package, 164, 165

Port Address Translation
 (PAT), 235

PowerShell commands, 242, 387

Private Branch Exchange
 (PBX), 32, 293

Private meetings, 270

Proof of concept (POC), 391

Public Safety Answering Point
 (PSAP), 92, 322

Q

Quality of Service (QoS) policies
 Active Directory container, 248
 application name, 253
 functions, 250
 implementation, 248
 IP addresses, 254
 media port ranges,
 configuration, 249
 name/DSCP values, 252
 source port number, 255
 verification, 256

R

Real-Time Messaging Protocol (RTMP), 22

Retention policies
 creation, 366–369
 managing, 365
 reviewing, 368
 Teams, 364

Reverse number lookup (RNL), 426

Role-based access control (RBAC), 428

Round robin method, 309

S

Sarbanes-Oxley (SOX) Act, 364

Serial routing, 309

Service numbers, 334

Session border controller (SBC), 32

Session Initiation Protocol (SIP), 460

SharePoint online, 9, 11

Sign-in process, 39

Single-factor authentication (SFA), 39

Single sign-on (SSO), 429

Skype for Business
 interoperability (*see* Native
 interoperability experience)
 migration process, 403, 404
 Online to Teams only mode, 422
 On-Premises Teams, 419–421
 prerequisites, 418, 419

Skype for Business Online
 CCE, 406
 Teams admin center, 404
 Windows PowerShell, 405

Split-tunnel VPN, 235
 architecture, 258
 Teams media traffic, 257, 258
 Teams traffic, 257

INDEX

Split-tunnel VPN (*cont.*)

third-party solution, 259–261

verification, 261, 262

Summary Reports tab, 217

Synchronized Identity, 16

System Center Configuration Manager
(SCCM), 58

T

Teams admin center, 76

access, 77

dashboard, 78

role, 77, 78

tab, 79

team/channel, 80

Team policies creation, 80–82

Teams and channels, 42

add member, 46

channel creation, 47, 50

add, 48

guest permissions, 55, 57

lock icon, 54

management settings, 55

member access, 56

privacy model, 49

private, 52–54

tabs, 51

create button, 44

create scratch, 45

general channel, 47

join, 43

name/description, 46

private/public, 45

Teams Apps tab, 114, 118

assign policy, 125, 126

blocking, 117

custom app, 120

custom app policy, 117

org-wide app settings, 116

Permission policies, 114, 115

pinned apps, 123, 124

PowerShell, 124

setup policies, 120–122

users, 119

Teams Client login

process, 40, 41

Teams clients

all devices, 59

desktop/mobile, 58

management, 63

add-ins, 64

close, 65

configuration, 64

mobile, 66

uninstall, 63

update, 63

usage, 66, 67

software/hardware, 60

Windows, 60

installation, 61

MSI client, 62

MSI deployment, 62

Teams device usage report, 173, 174

Teams live events, 172, 173

Teams meetings

attendee types, 270

clients, 271

configuration, 275

delegation, 272

firewall configurations, 274, 275

licensing, 272

network considerations, 273

network segments, 274

policies assigned to users, 275, 276

recording, 272

- settings, 275
- users' experiences, 271
- Teams only experience, 411
 - Skype for Business experience after upgrade, 412, 413
- Teams org-wide settings, 175
- Teams reporting, 165, 168
- Teams Rooms, 88
 - administrative considerations, 89
 - create account, 90
 - Exchange Online, 89
- Teams settings, 186
- Teams usage report, 168
 - activity, 171
 - columns selection, 170
 - export, 169
 - users, 169
- Teams user activity report, 171
- Teams voice routing policies
 - number pattern, 336
 - PSTN gateway, 338
 - PSTN usage, 337
- Telemetry, 7
- Third-party application
 - app permission policies, 346
 - assigning custom app setup policies, 347
 - functionality, 345
 - managing custom app setup policies, 346
 - Teams apps/policies, 346
- Transmission Control Protocol (TCP), 22, 254
- Transport Layer Security (TLS), 297

U

- User Datagram Protocol (UDP), 254
- User migration

- end-to-end security, 389
- end users, 388
- network environment, 389
- operational part, 423
- optimal audio/video quality, 388
- process, 423
- robust platform, 388
- Skype for Business (*see* Skype for Business Online)
 - tips, 418
- User phone numbers, 335
- User principal name (UPN), 38
- User provisioning
 - assign/remove policy, 343–345
 - enabling license, 342
- Users tab, 98

V

- Virtual Desktop Infrastructure (VDI), 66
- Virtual private network (VPN), 231
- Voicemail, 7
- Voice over IP (VoIP), 4
- Voice tab, 126
 - Advisor, 204
 - call park (*see* Call park policy)
 - custom dial plan, 140
 - dial plan, configuration, 139–141
 - emergency calling policies, 129–131
 - emergency numbers, 136
 - network, 133
 - network site, 138
 - phone number
 - management, 127, 128
 - planning, 204
 - porting, phone number, 128, 129
 - PowerShell, 132, 137, 138

INDEX

Voice tab (*cont.*)

- routing policies, [133–135](#)
- Teams admin center, [130](#), [131](#)
- user, group, [132](#)
- users, [144](#)
- Windows PowerShell, [145](#), [146](#)

W, X, Y, Z

- Wide-area network (WAN), [232](#)
- Wi-Fi Multimedia (WMM), [234](#)
- Windows Teams client, [40](#)
- Wireless access points (WAPs), [330](#)