DUMPSARENA

Managing Microsoft Teams

Microsoft MS-700

Version Demo

Total Demo Questions: 65

Total Premium Questions: 657

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Configure and manage a Microsoft Teams environment	125
Topic 2, Manage chat, calling, and meetings	222
Topic 3, Manage teams, channels, apps, and files	193
Topic 4, Monitor and troubleshoot a Microsoft Teams environment	63
Topic 5, Mix Questions	3
Topic 6, Case Study Contoso, Ltd	26
Topic 7, Case Study Litware, inc	12
Topic 8, Case Study A. Datum Corporation	13
Total	657

QUESTION NO: 1

Your organization consists of 200 users, and you are planning to transition all users from Microsoft Skype for Business Online to Microsoft Teams. It is essential to enable Phone System with Teams for every user. You need to propose the appropriate coexistence mode in the Microsoft Teams upgrade policy to facilitate this transition. Which coexistence mode should you recommend to ensure a smooth upgrade?

A. Skype for Business with Teams collaboration

B. Islands

C. Teams only

D. Skype for Business with Teams collaboration and meetings

ANSWER: C

Explanation:

Teams only is the appropriate coexistence mode because the organization is completing its transition from Skype for Business Online to Teams and requires Teams Phone capabilities for every user. This mode is Microsoft's intended final upgrade state: Teams becomes the sole client for chat, calling, meetings, and collaboration. It provides a consistent experience in which users place and receive calls through Teams rather than having calling workloads split across Skype for Business and Teams.

For users enabled for Phone System, Teams only supports Teams-based enterprise calling with a PSTN connectivity option, including Microsoft Calling Plan, Operator Connect, or Direct Routing. During the transition, administrators can assign Teams only through the Teams upgrade policy on a per-user basis or tenant-wide when the organization is ready. Microsoft also supports migrating eligible Skype for Business Online users to Teams, which moves them to Teams only as part of the upgrade. This aligns the communications client, calling configuration, and user experience with the organization's stated end state. See Microsoft's Teams upgrade and coexistence guidance and Teams Phone configuration guidance.

QUESTION NO: 2

Your company is in the process of transitioning from Microsoft Skype for Business Online to Microsoft Teams. Currently, the organization's Microsoft Teams upgrade policy is set to the Islands coexistence mode, and there is an intention to retain this mode for an extended period. Some users have reported receiving email notifications about missed chat communications. You need to propose a solution to ensure all users receive their chat messages effectively. Which two actions should you suggest? Each correct answer is a part of the complete solution. NOTE: Each correct selection is worth one point.

A. Install the Microsoft Teams clients on all the computers that run the Skype for Business client. Instruct the users to sign in to both client applications.

B. Instruct the users to modify the permissions in the Microsoft Teams client.

C. Modify the global app setup policy.

D. Modify the global app permission policy.

E. Install the Skype for Business client on all the computers that run the Microsoft Teams client. Instruct the users to sign in to both client applications.

ANSWER: A E

Explanation:

In Islands mode, Microsoft Teams and Skype for Business are independent communication clients. A chat that is initiated in Teams is delivered to the recipient's Teams client, while a chat initiated in Skype for Business is delivered to that user's Skype for Business client. Because the organization intends to remain in Islands mode, users must have access to—and remain signed in to—both clients to receive chats consistently, irrespective of which client the sender uses. Installing the Microsoft Teams clients on all the computers that run the Skype for Business client and instructing users to sign in to both applications provides Teams message delivery on devices previously used only for Skype for Business. Likewise, installing the Skype for Business client on all the computers that run the Microsoft Teams client and instructing users to sign in to both

applications ensures that Skype for Business chats are not missed on Teams-oriented devices. Together, these actions give users active presence and message notifications in each separate service, avoiding reliance on delayed missed-message email notifications. Microsoft recommends careful user education when Islands mode is retained because users must understand that chats and calls can arrive in either client. See Teams and Skype for Business coexistence and interoperability and coexistence and upgrade settings.

QUESTION NO: 3

You are working as a Systems Administrator at your company which has a subscription to Microsoft 365. All users in the organization are equipped with a Microsoft 365 E3 license and utilize Microsoft Teams for collaboration. According to the company's security policy, it is mandatory that all files used in personal chats or team collaborations be retained for at least one year. Your task is to configure a retention policy to conform to this security requirement. Which two locations should the retention policy be applied to in order to adhere to this policy? (Choose two).

A. OneDrive accounts

B. Exchange email

C. Teams chat

D. SharePoint sites

E. Teams channel messages

ANSWER: A D

Explanation:

OneDrive accounts and **SharePoint sites** are the required retention-policy locations because Teams stores files in those Microsoft 365 services rather than in the Teams messaging workload. Files uploaded and shared in one-to-one chats or group chats are stored in the OneDrive account of the person who uploaded them, ordinarily in the *Microsoft Teams Chat Files* folder. A retention policy scoped to OneDrive therefore retains chat files for the required one-year period, including when users later delete the files.

Files uploaded to standard channels are stored in the document library of the SharePoint site associated with the team. Scoping the policy to SharePoint sites retains files used for channel-based team collaboration. For complete coverage of the stated requirement, configure the applicable retention settings for both services and retain content for at least one year. Microsoft's Teams file-storage documentation describes the OneDrive storage location for chat files and SharePoint storage location for channel files. Microsoft Purview retention policies can be applied to SharePoint and OneDrive to retain this content in place or preserve it through the retention process. See Share files in Microsoft Teams and Learn about retention for SharePoint and OneDrive.

QUESTION NO: 4

Scenario:

Your company subscribes to Microsoft 365. You need to ensure that a user, referred to as User1, is unable to permanently delete private chats in Microsoft Teams.

Solution: Implement an In-Place Hold on the Microsoft SharePoint site utilized by Microsoft Teams.

Is this approach effective in achieving the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Private chats in Microsoft Teams are not stored in the SharePoint site used by a team. For compliance and retention purposes, copies of one-to-one and group chat messages are stored as hidden email messages in the Exchange Online mailboxes of the chat participants. The SharePoint site associated with a team is principally a storage location for files shared in standard channels, so a hold scoped only to that site does not preserve private-chat messages.

To ensure that chat content remains available after a user deletes it from the Teams client, the organization should configure Microsoft Purview retention for Teams chats. A retention policy can be scoped to Teams chat messages and to the required users, including User1. Retained chat messages are preserved in the relevant Exchange Online mailbox for the configured retention period, supporting compliance requirements independently of the user-facing deletion action. Microsoft's Teams retention guidance describes how Purview retention policies retain chat messages, and its Teams data-location documentation confirms the Exchange Online storage location for chat compliance records. See Learn about retention for Microsoft Teams and Location of data in Microsoft Teams.

QUESTION NO: 5

You have a Microsoft 365 subscription and are planning to implement Microsoft Teams. To ensure optimal network performance, you need to conduct network quality and connectivity tests from your on-premises network to Microsoft 365 Online services using the Network Testing Companion tool. You have already installed the Network Testing Companion module on a local Windows 10 device. What is the next software you should install to complete the tests successfully?

A. the Microsoft Teams desktop client

B. Network Assessment Tool

C. Windows Assessment Toolkit

D. Windows Performance Analyzer (WPA)

ANSWER: B

Explanation:

Network Assessment Tool is the required software because the Network Testing Companion PowerShell module depends on the Microsoft Network Assessment Tool to perform the actual network measurements. The companion module provides PowerShell-based orchestration and reporting, while the assessment tool supplies the executable that tests the client's connectivity path to Microsoft 365 and measures real-time media network characteristics. Installing it on the Windows device enables collection of metrics that are important when assessing readiness for Teams calling and meetings, including latency, packet loss, jitter, and connectivity to relevant Microsoft service endpoints.

Running these tests from the on-premises network is important because Teams media quality is strongly affected by the actual network path used by client devices, rather than merely by the organization's available internet bandwidth. The results help administrators identify whether local network configuration, egress routing, or connectivity behavior should be addressed before deployment. Microsoft provides the Network Assessment Tool download at Network Assessment Tool. For current Teams network-planning guidance and recommendations for validating connectivity and media performance, see Prepare your organization's network for Microsoft Teams.

QUESTION NO: 6

You are employed as a Microsoft 365 Administrator within your organization where all employees have been assigned Microsoft 365 E5 licenses. Microsoft Teams is the primary tool used by staff for collaboration purposes.

Recently, you have uploaded a custom application to Microsoft Teams that is intended for company-wide use. Your objective now is to ensure that this custom application is prominently placed at the top of the app bar in Microsoft Teams for all users.

Which of the following actions should you take to accomplish this goal?

A. Configure the global app setup policy.

B. Create a configuration profile.

C. Configure the global app permission policy.

D. Configure the global Teams policy.

ANSWER: A

Explanation:

Configure the global app setup policy. In Microsoft Teams, app setup policies control the apps that are installed and pinned for users, including the order in which pinned apps are displayed on the Teams app bar. After the custom app has been uploaded and is permitted for use in the tenant, an administrator can edit the global app setup policy in the Teams admin center, add the custom app to the pinned apps list, and place it at the top of that list. This ensures that the app is prominently presented to users who receive the global policy. The global app setup policy is the organization-wide default, making it the appropriate policy to configure when the intent is broad deployment rather than targeting a limited user group. If users are assigned a different app setup policy, that assigned policy takes precedence, so the organization should also ensure that no separate policy overrides the desired app pinning experience. Microsoft documents that app setup policies manage app installation and pinning behavior in Teams and can be used with organization-created custom apps. See Manage app setup policies in Microsoft Teams and Manage apps in the Teams admin center.

QUESTION NO: 7

You have a Microsoft 365 subscription that contains two users named User1 and User2. The users are provisioned for Microsoft Teams calling.

User1 is on leave for two weeks.

You need to ensure that User2 is notified of all calls to User1 while User1 is away.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Voice, add User2 to group call pickup.

B. From Voice, add User1 to group call pickup.

C. From Policies, modify the voice routing policy.

D. From the Microsoft Teams admin center, modify the settings of User2.

E. From the Microsoft Teams admin center, modify the settings of User1.

ANSWER: A E

Explanation:

From Voice, add User2 to group call pickup and, from the Microsoft Teams admin center, modify the settings of User1. Group call pickup is designed for a situation in which a designated colleague must be alerted to and able to answer calls placed to another user. The call pickup group is associated with the person whose calls need coverage—in this case, User1—so User1's voice settings are the location where the group is configured. Adding User2 as a member of that group causes calls ringing for User1 to be presented to User2, allowing User2 to answer them during the absence.

Configuring this arrangement in the Teams admin center enables an administrator to set up call handling on behalf of a user, which is particularly useful when the absent user cannot configure their own Teams client. The Voice area is also where the call pickup group membership is maintained; User2 must be added as a pickup member, rather than configuring a separate pickup group for User2. Microsoft documents group call pickup as a call-sharing feature that lets a user designate people who can receive and answer their calls. See Call sharing and group call pickup in Microsoft Teams and Manage call settings in Microsoft Teams.

QUESTION NO: 8

You have a Microsoft 365 subscription and you have created an organization-wide team named Team1. Users User1 and User2 own Team1. To configure Team1 to comply with the following requirements, which two actions should be taken through the Microsoft Teams client? Each correct action is part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Team1 settings, clear Give members the option to edit their messages

B. From the General Channel settings of Team1, set the channel moderation preference to Anyone can post; show alert that postings will notify everyone (recommended for large teams)

C. From the General Channel settings of Team1. set the channel moderation preference to Only owners can post messages.

D. From the Team1 settings, disable all the Fun stuff settings.

E. From the Team1 settings, set Show members the option to @team or @[team name] to Off.

ANSWER: C E

Explanation:

For an organization-wide team, restricting broad communications is important because the team can include nearly all users in the tenant. Setting the General channel moderation preference to *Only owners can post messages* makes the channel an owner-controlled announcement channel. Team owners can publish organization-wide information, while members can still read the channel content and receive the intended communications. Channel moderation is configured from the channel's management settings and is especially appropriate for the General channel of a large team.

Setting *Show members the option to @team or @[team name]* to Off prevents ordinary members from using a team mention that would notify the entire organization-wide team. This reduces unnecessary large-scale notifications while preserving the owners' ability to manage and communicate important updates. Together, owner-only posting in General and restricted team mentions provide controlled, low-noise communication for Team1. Microsoft documents the administration and considerations for organization-wide teams at Create an org-wide team in Microsoft Teams. Details on channel moderation, including limiting new posts to moderators, are available at Change moderation settings for a channel in Microsoft Teams.

QUESTION NO: 9

You have a Microsoft 365 ES subscription.

You plan to have Teams administrators use sell-help diagnostics.

Which two scenarios are covered by self-help diagnostics? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Validate that a specified user can disable Teams live events.

B. Validate that a specified user is configured to record meetings.

C. Review Teams guest access.

D. Attempt to locate a missing Teams meeting recording.

E. Validate end-to-end encryption for strictly confidential Teams meetings

ANSWER: B D

Explanation:

Teams self-help diagnostics in the Microsoft 365 admin center include meeting-recording troubleshooting scenarios. **Validate that a specified user is configured to record meetings.** is covered because the recording diagnostic evaluates the relevant user and meeting-recording configuration, such as the policies that determine whether recording is available to that user. This lets an administrator identify configuration issues affecting the user's ability to record a Teams meeting.

Attempt to locate a missing Teams meeting recording. is also covered. The missing-recording diagnostic helps administrators investigate recordings that users expect to find but cannot access. Its checks help establish the applicable recording storage location and identify common configuration or availability conditions that can affect access to a completed recording. These diagnostics are intended to provide targeted, tenant-aware troubleshooting through the Microsoft 365 admin center rather than requiring administrators to manually inspect every related setting. Microsoft documents the available Teams administrator diagnostics and also provides guidance specific to meeting-recording issues at Self-help diagnostics for Microsoft Teams administrators and Troubleshoot Teams meeting recording issues.

QUESTION NO: 10

Your organization has an active Microsoft Office 365 subscription. Members of the sales department often invite guest users to join meetings. You are tasked with ensuring that these guest users are automatically admitted to meetings organized by the sales department, without changing settings for other departments. What two steps would you take to achieve this goal? Each correct answer is a part of the complete solution.

Note: Each correct selection is worth one point.

A. In the global meeting policy, set Automatically admit users to Everyone.

B. Create a new meeting policy and set Automatically admit users to Everyone.

C. Apply the policy to the sales department users.

D. In the global meeting policy, set Automatically admit users to Everyone in your organization.

ANSWER: B C

Explanation:

Create a new meeting policy and set Automatically admit users to Everyone is correct because the lobby bypass behavior for a Teams meeting is governed by the meeting policy assigned to the meeting organizer. The *Everyone* setting allows meeting participants to bypass the lobby automatically, which includes guest users invited by sales organizers. Creating a dedicated policy provides a scoped configuration rather than modifying the tenant's default behavior.

Apply the policy to the sales department users is also required because policies affect meetings based on the policy assigned to the organizer, not based on the department of an attendee or the meeting invitation itself. Assigning the custom policy to the sales users makes the automatic-admission setting effective for meetings that they organize. The global meeting policy can therefore remain unchanged, preserving the existing lobby experience for organizers in other departments. Teams supports assigning a meeting policy directly to users or to a group, enabling this type of targeted departmental deployment. Microsoft documents the meeting-policy controls for lobby access and automatic admission in Meeting policies in Microsoft Teams, and documents targeted user and group policy assignment in Assign policies to users and groups.

QUESTION NO: 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has a Microsoft 365 subscription.

You plan to configure the environment to allow external users to collaborate in Microsoft Teams by using guest access.

The company implements a new security policy that has the following requirements:

Only guest users from specific domains must be allowed to connect to collaborate by using Microsoft Teams.

Guest users must be prevented from inviting other guests.

You need to recommend a solution to meet the security policy requirements.

Solution: From the Azure Active Directory, you modify the External collaboration settings.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes. Microsoft Entra ID external collaboration settings provide the tenant-level controls needed for both stated requirements. Under collaboration restrictions, an administrator can configure an allow list for invitation domains. When an allow list is used, invitations can be sent only to external users whose email domains are explicitly listed, which limits Teams guest collaboration to the approved organizations. This restriction is enforced when guest accounts are invited into the Microsoft 365 tenant, including when they are invited for Teams collaboration.

The same External collaboration settings area includes guest invite settings. An administrator can restrict who is permitted to invite guest users, such as limiting invitations to users in designated administrator roles or to specifically assigned roles. By not allowing guest users to invite, the organization prevents an existing guest from inviting additional external users while retaining the ability for authorized internal administrators or members to manage guest access as required.

These settings govern Microsoft Entra B2B collaboration, which is the identity and invitation foundation used by Teams guest access. The configuration therefore addresses domain-based guest restrictions and delegated guest-invitation control in one location. See Configure external collaboration settings and Collaborate with guests in a team.

QUESTION NO: 12

You have a Microsoft 365 E5 subscription that has Phone System enabled for all Microsoft Teams users.

You need to configure the Phone System to meet the following requirements:

▪ Provide a virtual receptionist that connects callers to either a specific user or the help desk. ▪ Route calls to the help desk on a First in, First out (FIFO) order.

Which two resources should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a call park policy

B. a call queue

C. a voice routing policy

D. a group call pickup

E. an auto attendant

F. a calling policy

ANSWER: B E

Explanation:

An auto attendant provides the virtual receptionist functionality required in this scenario. In Teams Phone, an auto attendant answers calls to an assigned resource account and phone number, plays a greeting, and presents menu options. Each menu choice can transfer the caller to an individual in the organization or to another call-handling destination, including a call queue. This enables callers to select either a specific user or the help desk through a single receptionist experience.

A call queue is the appropriate resource for the help desk because it holds incoming calls and distributes them to the help desk agents. Callers remain in the queue until an eligible agent is available, so calls are served in their arrival sequence. Teams supports several agent-routing methods, such as attendant, serial, round robin, and longest idle; these determine which available agent receives the next call, while the queue retains waiting callers in order. The auto attendant can therefore transfer the help-desk menu selection directly to the call queue, and the queue manages delivery to the help-desk staff.

Microsoft documents these resources as complementary Teams Phone capabilities: auto attendants handle greetings and call menus, while call queues route calls to groups of agents. See Plan for Teams auto attendants and call queues and Create a call queue in Microsoft Teams.

QUESTION NO: 13

You deploy a Teams Rooms device named Device 1.

You need to identify how many outbound meeting minutes were consumed during the last month by Device1.

Which report should you run?

A. Audio Conferencing dial-out usage

B. PSTN & SMS usage

C. Summary Reports

D. Rate My Call Reports

ANSWER: A

Explanation:

Audio Conferencing dial-out usage is the appropriate report because it records outbound calls made by users and devices through the Audio Conferencing service. A Teams Rooms device can place dial-out calls to add participants to a meeting, and those calls consume outbound Audio Conferencing minutes. The report provides call-level usage data, including the caller or resource account, dialed number, call date and time, duration, and applicable usage information. Administrators can use its date-range controls to select the previous month and then identify or filter the records associated with the resource account for Device1. The resulting call durations allow the administrator to determine the total number of outbound meeting minutes consumed by that room device during the selected period. This report is specifically intended for monitoring Audio Conferencing dial-out activity and associated consumption, making it suitable for reviewing a device's outbound meeting-minute usage. Microsoft documents the available Teams usage reports and their purposes in the Teams usage reports documentation. Additional details about managing and reviewing Audio Conferencing usage are available in the Audio Conferencing usage report documentation.

QUESTION NO: 14

You are managing a Microsoft 365 subscription for the domain contoso.com, which utilizes Microsoft Teams. Your objective is to enable Microsoft Teams users to perform the following functions:

Search for customers who use Skype (Consumer).
Initiate a Skype chat with these customers.

Which two actions should you take? Each correct answer forms part of the solution. NOTE: Each correct choice is worth one point.

A. From the Microsoft Teams admin center, turn on external access.

B. From the Azure portal, configure Azure AD B2C.

C. Add a _sipinternaltls SRV record to the contoso.com DNS domain.

D. From the Microsoft Teams admin center, turn on guest access.

E. Add a _sipfederationtls SRV record to the contoso.com DNS domain.

ANSWER: A E

Explanation:

From the Microsoft Teams admin center, turn on external access. is required because communication with Skype consumer users is controlled by the organization's Teams external-access configuration. An administrator must enable the setting that allows users in Teams to communicate with Skype users. Once this federation capability is enabled, Teams users can search for Skype consumer contacts by their Skype address and initiate one-to-one chats, subject to the supported external-communications experience and any applicable organizational policies. Microsoft describes the Skype consumer setting as part of Teams external access management: Manage external access in Microsoft Teams.

Add a _sipfederationtls SRV record to the contoso.com DNS domain. is also required for the organization's SIP federation configuration. The `_sipfederationtls._tcp` SRV record enables federation partners to discover the Microsoft-hosted service endpoint for the domain. Microsoft's DNS guidance lists this federation SRV record for domains using Skype for Business Online and Teams federation-related services. Correct DNS publication supports reliable discovery and routing of federated SIP communications for the organization's custom domain. The required target and record details are provided in Create DNS records at any DNS hosting provider.

QUESTION NO: 15

You have a Microsoft Office 365 subscription and you discover that apps from a third-party publisher are causing security concerns. What action should you take in the Microsoft Teams admin center to block all apps from this specific publisher?

A. Org-wide app settings

B. Policy packages

C. Permission policies

D. Manage apps

ANSWER: D

Explanation:

Manage apps is the appropriate area in the Microsoft Teams admin center because it is the central location for reviewing and controlling Teams apps at the organization level. It provides administrators with app inventory and publisher information, allowing them to identify the apps associated with a third-party publisher that has raised security concerns and change their availability status to blocked. Blocking these apps prevents them from being installed or used in Teams by users in the tenant, which is the direct administrative response to an identified app-publisher risk.

This control is part of Teams app governance. Administrators can use the app-management experience to assess app details, including the publisher, permissions, and status, then apply allow or block decisions that protect the organization while maintaining oversight of the Teams app ecosystem. The action is performed centrally and does not rely on individual users to remove or avoid the affected apps. Microsoft documents the app-management workflow and organization-level app availability controls in Manage apps in the Teams admin center. For broader governance context, see App management and governance in Teams.

QUESTION NO: 16

You have a Microsoft 365 subscription that includes Microsoft Teams.

You are planning to implement voice functionality in Microsoft Teams. To configure this, which two specific settings will necessitate the use of a resource account? Each correct answer is a part of the overall solution.

NOTE: Each correct selection is worth one point.

A. Call park policies

B. Auto attendant

C. Call queues

D. Emergency polices

E. Guest access

ANSWER: B C

Explanation:

Auto attendant and **Call queues** require resource accounts because these accounts provide the service identity used by Teams voice applications. A resource account is an Entra ID account that represents the application rather than an individual user. It is associated with an auto attendant or call queue and can be assigned a telephone number, enabling external and internal callers to reach that voice application.

For an auto attendant, the resource account is the endpoint callers use to reach the organization's automated greeting, menu choices, business-hours handling, and call-routing configuration. For a call queue, it is the endpoint through which incoming calls enter the queue before being distributed to the configured agents. An organization can use separate resource accounts and phone numbers for distinct auto attendants or queues, allowing each service to have its own callable identity.

When the resource account needs a phone number for Teams calling, the account must be licensed appropriately, such as with a Teams Phone Resource Account license where applicable. Microsoft's configuration guidance identifies resource accounts as the required accounts to create and associate with both auto attendants and call queues. See Manage resource accounts in Microsoft Teams and Plan for Teams auto attendants and call queues.

QUESTION NO: 17

Please note: This question is part of a series where each question shares the same scenario but contains a unique solution that may achieve the stated goals. Certain question sets may offer more than one correct solution, while others may not have a correct solution.

Once you respond to a question in this section, you cannot return to it, meaning these questions will not appear on the review screen.

Your organization holds a Microsoft 365 subscription.

You are tasked with preventing temporary employees from accessing the private chat feature in Microsoft Teams.

Solution proposed: Implement a meeting policy and assign this policy to the related users.

Does this solution satisfy the requirement?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. A Teams meeting policy does not control whether a user can use the general private-chat experience in Teams, such as one-to-one or group chats outside a meeting. Meeting policies manage capabilities specifically associated with meetings, including scheduling, lobby settings, media, recording, content sharing, and the meeting-chat experience. They therefore cannot be used to prevent temporary employees from accessing private chats throughout Teams.

To restrict private chat for a defined population such as temporary employees, the appropriate administrative control is a Teams messaging policy. Messaging policies contain the *Chat* setting, which determines whether users can use private chat. An administrator can create a dedicated messaging policy with chat disabled and assign it to the temporary employee accounts, either directly or through a supported group policy assignment method. This applies the restriction only to the intended users while leaving the organization's standard messaging experience in place for other employees. Microsoft

documents the chat setting and management of messaging policies at Manage messaging policies in Microsoft Teams. For supported methods of applying the tailored policy to users or groups, see Assign policies to users and groups in Teams.

QUESTION NO: 18

Your organization subscribes to Microsoft 365, and this includes a subscription for 200 Microsoft Teams users, with a specific team called IT Support consisting of 50 members.

Your objective is to configure the caller ID for outgoing PSTN calls made by the IT Support team so that it displays the phone number of the company's IT helpdesk. You must achieve this with minimal administrative overhead.

Which two tools should be part of your solution? Each correct tool contributes to solving the requirement.

NOTE: Each correct choice is worth one point.

A. the Microsoft Teams PowerShell module

B. the Azure Active Directory (Azure AD) PowerShell for Graph module

C. the Call Quality Dashboard (CQD)

D. the Windows PowerShell module for Microsoft Skype for Business Online

E. the Skype for Business admin center

F. the Microsoft Teams admin center

ANSWER: A F

Explanation:

The Microsoft Teams admin center is used to create and manage caller ID policies for Teams Phone. A caller ID policy can replace a user's outbound PSTN caller ID with a specified service number or resource account number. Therefore, the IT helpdesk telephone number can be configured as the number presented when members of IT Support place external calls. This central configuration ensures that callers see a consistent organizational contact number and can return calls to the helpdesk rather than to an individual employee.

The Microsoft Teams PowerShell module is also part of the solution because it enables policy assignment to a group. The IT Support team is backed by a Microsoft 365 group, so assigning the caller ID policy to that group avoids manually assigning it to each of the 50 members. Group-based assignment substantially reduces administration and also helps apply the required policy to relevant group members as membership is managed. Microsoft documents caller ID policy configuration and supported substitutions in Manage caller ID policies in Microsoft Teams. Policy assignment capabilities, including group assignment through Teams PowerShell, are documented in Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 19

Note: This question is part of a series where each question presents the same scenario. Each question in this series contains a unique solution that might achieve the stated goals. Some sets of questions may have more than one correct solution, while others may not have a correct solution. After responding to a question in this section, you will NOT be able to return to it. Therefore, these questions will not appear in the review screen.

Your organization has a Microsoft 365 subscription that utilizes an Azure Active Directory (Azure AD) tenant named contoso.com. You need to ensure that guest users within the tenant are restricted from using cameras during Microsoft Teams meetings.

Proposed Solution: Modify the External sharing settings from the Microsoft Teams admin center.

Does this approach fulfill the requirement?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Modifying External sharing settings in the Teams admin center does not control whether guests can turn on their cameras during Teams meetings. External access and guest access settings govern the organization's collaboration boundaries and the capabilities available to external participants and guests at a broad level; they are not the configuration surface for meeting-media controls such as camera use.

Camera availability in a Teams meeting is governed by Teams meeting policy audio and video settings. An administrator can create or modify a meeting policy that disables IP video, then assign that policy to the relevant guest users. Microsoft's meeting-policy documentation identifies the *IP video* setting as the control that determines whether users can turn on video in meetings. Therefore, because the proposed change addresses external sharing rather than the applicable meeting policy, it does not fulfill the stated requirement.

For the relevant policy setting and assignment guidance, see Manage meeting policies for audio and video in Microsoft Teams. Microsoft's separate guidance on guest collaboration is available at Collaborate with guests in a team.

QUESTION NO: 20

Your organization receives reports that a user experienced poor audio quality in a specific Teams call yesterday.

You need to investigate the individual call and also determine whether the issue represents a broader quality trend for users at the same office location.

Which two tools should you use? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. Call Analytics

B. Call Quality Dashboard (CQD)

C. The Microsoft 365 Groups activity report

D. Teams advisor

E. The Teams device usage report

ANSWER: A B

Explanation:

Use **Call Analytics** to investigate the individual user's call. Call Analytics provides per-call and per-meeting details that help administrators investigate media quality for a specific participant and session. The data can include stream information, network metrics, device information, and call-quality indicators.

Use **Call Quality Dashboard (CQD)** to analyze broader trends. CQD aggregates call and meeting quality data across the organization and supports filtering and grouping by dimensions such as building, network, subnet, and date. This makes it suitable for determining whether the problem affects multiple users at the same office.

Microsoft documents individual-call troubleshooting in Use Call Analytics to troubleshoot poor call quality and organization-wide analysis in Use Call Quality Dashboard for Microsoft Teams.

QUESTION NO: 21

Your company has a Microsoft 365 subscription that contains three groups named HR, Marketing, and Sales.

You need to configure the Microsoft Teams desktop client. The solution must meet the following requirements:

Members of the HR group must be prevented from pinning apps to their app bar.

Members of the Marketing group must have the Microsoft Planner app pinned to their app bar.

Members of the Sales group must not be affected by policies applied to the Marketing and HR groups.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Modify the global app setup policy.

B. Modify the global app permission policy.

C. Create an app setup policy for HR.

D. Create an app setup policy for Marketing.

E. Create an app permission policy for Marketing.

F. Create an app permission policy for HR.

ANSWER: C D

Explanation:

Creating an app setup policy for HR provides the policy container needed to control the Teams app bar experience for HR users. In that policy, the administrator can disable user app pinning, preventing those users from adding their own apps to the app bar. The policy can then be assigned to the HR group, which scopes the setting to its members rather than applying it across the tenant.

Creating an app setup policy for Marketing separately enables a tailored pinned-app configuration for Marketing users. The administrator can add the Planner app to that policy's pinned-app list, causing it to appear in the app bar for members who receive the policy. Teams supports app setup policies specifically for defining the apps that are pinned in the client and for controlling whether users can pin apps themselves.

Using separate policies and assigning each only to its intended Microsoft 365 group isolates the configurations. Consequently, Sales users remain on the effective policy otherwise applicable to them and do not inherit the HR restriction or Marketing pinned-app configuration. For Microsoft's guidance on configuring app setup policies and managing pinned apps, see Manage app setup policies in Microsoft Teams. For group-based assignment of Teams policies, see Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 22

You are a Microsoft 365 Administrator for your organization where every user is provided with Microsoft 365 licenses. Users often engage in private chats using Microsoft Teams for collaboration. Your task is to ensure that a particular user is restricted from permanently deleting private chats. Which option should you configure to achieve this?

A. The user's Microsoft 365 license options in the Microsoft 365 Admin Center.

B. A meeting policy in Microsoft Teams.

C. A litigation hold on the user's mailbox.

D. A Sensitivity Label in the Security & Compliance Admin Center.

ANSWER: C

Explanation:

A litigation hold on the user's mailbox is the appropriate configuration because Teams private-chat messages are journaled to hidden folders in the Exchange Online mailboxes of the chat participants for compliance, eDiscovery, and retention purposes. Applying Litigation Hold to the particular user's mailbox preserves mailbox content for the defined hold duration, including items that the user deletes and the original versions of items that are modified. Therefore, deletion of a private-chat message through the Teams client does not permanently remove the compliance copy from the organization's Exchange

Online data store. The retained content remains discoverable through Microsoft Purview eDiscovery for the duration of the hold, which satisfies the requirement to ensure that this user cannot permanently erase relevant private-chat data. Litigation Hold is applied at the mailbox level and is suited to an individual user when a legal, investigative, or compliance requirement requires preservation of their communications. Microsoft's Teams eDiscovery guidance confirms that Teams chat content is stored in Exchange mailboxes, while Exchange Litigation Hold documentation describes how held mailbox items are retained even after deletion. See eDiscovery of Teams content and Litigation holds in Exchange Online.

QUESTION NO: 23

Your organization has an active Microsoft 365 subscription, with all members assigned a Microsoft 365 E3 license.

There is a need to establish information barriers between two distinct groups of users within the organization.

Which two licensing add-ons are necessary to achieve this functionality? Each correct selection provides a complete solution.

Each correct selection is worth one point.

A. Microsoft Defender for Office 365

B. Microsoft 365 E5 Insider Risk Management

C. Microsoft 365 E5 Compliance

D. Communications Credits

ANSWER: B C

Explanation:

Microsoft 365 E5 Insider Risk Management and Microsoft 365 E5 Compliance are the appropriate add-ons for an organization that has Microsoft 365 E3 and needs to deploy Microsoft Purview Information Barriers. Information Barriers is a Purview compliance capability used to prevent communication and collaboration between defined user segments. For example, an organization can prevent users in one business group from finding, chatting with, calling, or collaborating with users in another group where regulatory, ethical-wall, or confidentiality requirements apply. Policies can be enforced across supported Microsoft 365 services, including Teams, SharePoint, and OneDrive.

Microsoft documents Information Barriers licensing as being available through eligible Microsoft 365 and Office 365 E5 offerings, including the E5 Compliance and E5 Insider Risk Management add-ons. Therefore, either qualifying add-on can extend a Microsoft 365 E3 deployment with the required entitlement for users who need Information Barriers functionality. Licensing must be assigned appropriately to users who are included in Information Barrier segments or otherwise benefit from the capability, consistent with Microsoft's licensing guidance. For implementation details and licensing requirements, see Microsoft Purview Information Barriers and Information Barrier policies.

QUESTION NO: 24

You have a Microsoft 365 subscription which includes two users, User1 and User2, who are both set up for Microsoft Teams calling.

User1 will be on leave for two weeks and you are required to ensure that User2 receives notifications for all calls directed to User1 during this period.

Which **two** actions should be taken to accomplish this task? Each correct answer forms a part of the solution.

Note: Each correct selection is worth one point.

A. From Voice, add User2 to group call pickup.

B. From Voice, add User1 to group call pickup.

C. From Policies, modify the voice routing policy.

D. From the Microsoft Teams admin center, modify the settings of User2.

E. From the Microsoft Teams admin center, modify the settings of User1.

ANSWER: A E

Explanation:

“From Voice, add User2 to group call pickup.” is correct because User1’s call group must contain User2 before User2 can receive the shared incoming-call alert and answer a call placed to User1. In Teams, this capability is called call sharing and group call pickup. It enables a user to designate other people to receive alerts for their incoming calls, which is appropriate for temporary cover during leave.

“From the Microsoft Teams admin center, modify the settings of User1.” is also correct because the relevant call-handling configuration belongs to the person whose calls are being covered: User1. An administrator can manage a user’s call settings and configure the incoming-call rule to simultaneously ring the call group or forward calls to it. Combining the group membership with User1’s call-answering rule ensures that calls originally directed to User1 generate notifications for User2 for the required period. Microsoft documents the call-group behavior, including shared alerts and answering calls for another user, in its Call sharing and group call pickup documentation. Administrative management of the user-level calling configuration is described in Manage user call settings in Teams.

QUESTION NO: 25

Your company subscribes to Microsoft 365, and the Microsoft 365 tenant is configured with the domain contoso.com. You need to configure the team channels to only accept emails from users within your company and email addresses that utilize the @fabrikam.com domain. Which setting should you modify?

A. the External collaboration settings in the Azure Active Directory admin center

B. the list of accepted domains in Microsoft Exchange Online

C. the Teams settings

D. the global teams policy

ANSWER: C

Explanation:

The Teams settings is correct because channel email is governed by an organization-wide Teams email integration configuration. In the Teams admin center, an administrator can enable email integration for channels and define the SMTP domains from which Teams channels can receive email. This allows the organization to permit messages originating from its own users while also explicitly allowing messages sent from the fabrikam.com domain. The configuration applies to Teams channel email addresses, rather than to general Exchange mail flow or collaboration invitations, so it directly controls the requested channel-level inbound email behavior. Administrators access this setting in the Teams admin center under **Teams settings**, in the Email integration area, where they can specify the allowed SMTP domains. Adding fabrikam.com to that list establishes the required external-domain exception while preserving the organization’s intended restrictions for other senders. Microsoft documents that Teams channel email can be enabled and restricted by accepted SMTP domains in its Teams email integration guidance. For implementation details, see Email integration in Teams settings and Send email to a channel in Microsoft Teams.

QUESTION NO: 26

You need to configure the user accounts of the sales department users to meet the security requirements.

What should you do for each user?

A. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName SfBWithTeamsCollabAndMeetings cmdlet.

B. From the Microsoft Teams admin center, set the Microsoft Teams upgrade policy to **Islands** coexistence mode.

C. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName Islands cmdlet.

D. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName SfBOnly cmdlet.

ANSWER: A

Explanation:

Run `Grant-CsTeamsUpgradePolicy -PolicyName SfBWithTeamsCollabAndMeetings` for each sales user. This command assigns the Teams upgrade (coexistence) policy directly to the specified user, allowing the organization to apply a different coexistence configuration to the sales department than to the tenant default or other users. The `SfBWithTeamsCollabAndMeetings` mode keeps Skype for Business as the user's service for presence, instant messaging, and calling, while enabling Teams for collaboration features such as channels, files, apps, and Teams meetings. Assigning the policy at the user level is appropriate when the requirement applies specifically to a defined department rather than every user in the organization. The command is used with an identity parameter for each target account, for example: `Grant-CsTeamsUpgradePolicy -Identity user@contoso.com -PolicyName SfBWithTeamsCollabAndMeetings`. Microsoft documents this coexistence mode and its workload behavior in the Teams and Skype for Business coexistence guidance. The available parameters and usage for assigning this policy are documented in the Grant-CsTeamsUpgradePolicy reference.

QUESTION NO: 27

Note: This question is part of a series where each scenario may have distinct goals and unique solutions. Once answered, you cannot revisit it. These questions will not appear in your review screen.

Your organization holds a Microsoft 365 subscription.

You are tasked with ensuring that temporary employees are restricted from utilizing the private chat function in Microsoft Teams.

Proposed Solution: Implement an app permission policy and assign this policy to the respective users.

Does this solution achieve the stated objective?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. An app permission policy governs access to Teams apps, including Microsoft-provided, third-party, and custom apps; it does not control core Teams chat functionality. Restricting private chat for a defined population, such as temporary employees, requires a Teams messaging policy assigned to those users. The messaging policy includes the *Chat* setting, which controls whether users can use private chat in Teams. An administrator can create a custom messaging policy with chat disabled, assign it to the temporary employees, and thereby prevent those users from participating in private one-to-one or group chats while applying the restriction only to the intended group. This is a user-level policy assignment scenario rather than an app availability scenario. Microsoft documents the chat setting as part of Teams messaging policies and documents app permission policies separately for managing which apps users can access. For configuration details, see Manage messaging policies in Teams and Manage app permission policies in Teams.

QUESTION NO: 28

Your company has a Microsoft 365 subscription.

A user invites an external user to join a Microsoft Teams meeting by using a Microsoft Outlook meeting

invitation.

The external user cannot join the meeting.

You need to ensure that all external users can join Microsoft Team meetings.

What should you do from the Microsoft Teams admin center?

A. From Guest access in the Org-wide settings, set Allow guest access in Microsoft Teams to On .

B. Edit the Meeting settings and set Anonymous users can join a meeting to On .

C. Edit the global meeting policy and set Allow scheduling private meetings to On .

D. Edit the live events policy and set Who can join live events to Everyone .

ANSWER: B

Explanation:

Enable **Anonymous users can join a meeting** in the Teams admin center under the organization-wide meeting settings. This tenant-level control permits people outside the organization who do not authenticate with an account in the tenant to use a Teams meeting link and enter the meeting as anonymous participants. An Outlook invitation for a Teams meeting includes the meeting join link, and an external recipient can use that link without being configured as a Teams guest, provided anonymous meeting access is enabled.

This setting is appropriate for the requirement because it applies broadly to externally invited meeting attendees, including recipients using personal accounts, accounts from other organizations, or no signed-in Teams identity. After joining, such attendees can still be held in the lobby according to the organizer's meeting options and applicable meeting policies; enabling anonymous join authorizes access to the meeting experience rather than bypassing organizer controls. Microsoft documents anonymous participant access as an organization-wide meeting setting in the Teams admin center. See Meeting settings in Microsoft Teams and Manage anonymous participant access to Teams meetings.

QUESTION NO: 29

This question is part of a series where the same scenario is presented. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others may have none. Once you answer, you will NOT be able to return to the question. As such, these questions will not appear in review screens.

Your company has a Microsoft 365 subscription and utilizes a Virtual Desktop Infrastructure (VDI) solution. The upgrade policy for Microsoft Teams within the company is set to 'Teams only' coexistence mode.

The Microsoft Installer (MSI) package for Microsoft Teams has been deployed to the VDI solution. However, months later, users report missing several new Microsoft Teams features on their workstations.

To ensure these VDI solution users have access to the latest Microsoft Teams features, a solution is proposed: Modify the Microsoft Teams upgrade policy through the admin center.

Does this solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. The Teams upgrade policy in the Teams admin center governs coexistence behavior and the transition experience between Skype for Business and Teams. For example, the *Teams only* mode determines that Teams is the primary communications client for users. This policy setting does not deploy a newer Teams desktop client, update an MSI-installed client in a virtual desktop image, or make client capabilities available when those capabilities depend on a more recent client build.

For a VDI deployment, client currency must be handled through the organization's image-management and software-deployment process. Since the Teams MSI package was deployed months earlier, the VDI image or installation mechanism needs to be updated with an appropriate current Teams client release so that users receive the features included in that release. Microsoft's VDI guidance describes the client installation and optimization considerations that administrators must account for in virtualized environments. Microsoft also documents that Teams client updates are managed separately from Teams upgrade and coexistence policies. Therefore, changing the upgrade policy does not meet the goal of providing these VDI users with the latest Teams features.

See Teams for Virtualized Desktop Infrastructure and Teams client update.

QUESTION NO: 30

Your company has 10 offices in North America and Europe.

The company has 5,000 users.

You plan to deploy Microsoft Teams for all the users.

You run a pilot project for the planned deployment.

You need to identify the network packet loss from the pilot computers to Microsoft Teams during calls.

Solution: From the Microsoft Teams admin center, you review Usage reports.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Teams usage reports provide organization-level information about service usage and adoption, such as user activity, chat messages, channel messages, meetings, calls, and device usage. They are useful for monitoring whether Teams is being adopted during a pilot, but they do not expose the per-call media telemetry needed to identify packet loss between pilot computers and the Teams service.

Packet loss is a call-quality measurement. To investigate it, Teams administrators should use Call Analytics for detailed diagnostics on a specific user or call. Call Analytics includes audio, video, and screen-sharing stream information, along with network measurements such as packet loss, jitter, round-trip time, and connection details. This lets the administrator identify whether a pilot participant experienced network impairment during a particular call. For broader pilot validation across offices, the Call Quality Dashboard can also be used to analyze aggregate call-quality patterns by location, network, device, and time period.

Therefore, reviewing Usage reports alone does not meet the stated goal of identifying network packet loss during calls. For Microsoft's reporting and call-quality guidance, see Teams reporting reference and Use Call Analytics to troubleshoot poor call quality.

QUESTION NO: 31

You are planning to deploy Microsoft Teams to a remote location and have conducted a network readiness assessment using the Network Testing Companion for Microsoft Teams. Which two of the following tests are included in the assessment? Each correct answer contributes to part of the overall solution. Note that each correct selection is worth one point.

A. video quality tests

B. trace route information

C. Quality of Service (QoS) validation

D. open and blocked ports

E. audio quality tests

ANSWER: D E

Explanation:

open and blocked ports and **audio quality tests** are included in the network readiness assessment. Teams relies on specific network connectivity paths and ports for its real-time media workloads. Validating that the required ports are available helps identify firewall or network-device configurations that could prevent clients at the remote location from establishing Teams media sessions. This is a core deployment-readiness activity because calls and meetings require reliable access to Microsoft media services.

The assessment also evaluates audio-media performance. The Network Assessment Tool component simulates real-time audio traffic and captures network measurements that affect the user experience, including latency, jitter, packet loss, and packet reordering. These measurements help an organization establish whether the location can support acceptable Teams calling and meeting audio before users are migrated or enabled. Microsoft recommends assessing network performance, connectivity, and firewall readiness for each site, particularly remote and branch offices, before deploying Teams. See Prepare your organization's network for Microsoft Teams and Network Assessment Tool.

QUESTION NO: 32

You have a Microsoft 365 subscription with two users, User1 and User2, who are both configured for Microsoft Teams calling. User1 is scheduled to be on leave for two weeks. Your task is to make sure User2 receives notifications for all calls directed to User1 during this period. What two actions should you take to achieve this? Each correct answer is part of the overall solution.

Note: Each correct selection is worth one point.

A. From Voice, add User2 to group call pickup.

B. From Voice, add User1 to group call pickup.

C. From Policies, modify the voice routing policy.

D. From the Microsoft Teams admin center, modify the settings of User2.

E. From the Microsoft Teams admin center, modify the settings of User1.

ANSWER: A E

Explanation:

From Voice, add User2 to group call pickup and, from the Microsoft Teams admin center, modify the settings of User1. These actions configure the call recipient’s call-answering behavior while making User2 available to receive and answer calls on that user’s behalf. User1 is the original recipient of the incoming calls, so the applicable call settings must be configured on User1’s account. An administrator can manage a user’s call-answering rules in the Teams admin center, including simultaneous ringing, forwarding, delegation, call groups, and unanswered-call handling. For the leave period, the rule can be configured so User2 is notified when a call arrives for User1. Adding User2 to group call pickup establishes User2 as the colleague who can receive or pick up User1’s calls under the configured arrangement. Together, the group membership and User1’s call settings ensure that incoming calls remain directed to User1’s number but are surfaced to User2 for timely response. Microsoft documents the available user-level calling controls in Manage user call settings in Microsoft Teams. The PowerShell configuration model likewise applies calling settings to the user whose calls are being handled, as described by Set-CsUserCallingSettings.

QUESTION NO: 33

Your company is subscribed to Microsoft 365. You need to enable collaboration between users from a partner company, Contoso, Ltd., and your company's users in Microsoft Teams. The solution should allow Contoso's users to exchange chat messages within the Teams channels.

What are the three necessary actions you must take before adding the Contoso users to Teams? Each correct answer contributes to the overall solution.

NOTE: Each correct selection is worth one point.

A. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group members outside the organization access group content to On.

B. From the Guest access settings in the Microsoft Teams admin center, set Allow guest access in Microsoft Teams to On.

C. From the External collaboration settings in the Azure Active Directory admin center, add Contoso's domain to the list of target domains.

D. From the External access settings in the Microsoft Teams admin center, add Contoso's domain to the Allowed list of domains.

E. From the External collaboration settings in the Azure Active Directory admin center, set Guest users permissions are limited to No.

F. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group owners add people outside the organization to groups to On.

ANSWER: A B F

Explanation:

To participate in channel conversations, Contoso users must collaborate as guest users in a team. Teams guest access must therefore be enabled by setting *Allow guest access in Microsoft Teams* to On. This is the Teams tenant-level control that permits guests to be added to teams and use the guest capabilities available in Teams, including participation in channel conversations.

Every team is backed by a Microsoft 365 group, so the Microsoft 365 Groups guest settings must also support external membership. Setting *Let group owners add people outside the organization to groups* to On permits team owners to add Contoso users as guests through the team's underlying group. Setting *Let group members outside the organization access group content* to On then gives those guest members access to the group-backed resources used for team collaboration, including the team's channels and associated content.

These settings form the core Microsoft 365 Groups and Teams configuration required before the external users can be added as guests to the relevant team. Microsoft documents the required tenant configuration in its Guest access in Microsoft Teams guidance and its guest access checklist.

QUESTION NO: 34

You have a Microsoft 365 subscription that includes Microsoft Teams.

A user reports encountering an error when attempting to share their screen during meetings using the Microsoft Teams Windows Desktop client.

To troubleshoot, you need to gather the Microsoft Teams client log files from the user's device.

What action should you take?

A. From the Microsoft Teams client settings, select Disable GPU hardware acceleration.

B. Select Ctrl + Alt + Shift + 1.

C. Select the Windows logo key + Alt + Shift +1

D. From the Microsoft Teams client settings, select Enable logging for meeting diagnostics.

ANSWER: B

Explanation:

Select Ctrl + Alt + Shift + 1. This is the Microsoft-documented keyboard shortcut for collecting diagnostic logs from the Teams desktop client on Windows. The user should invoke it while the Teams client is open, which causes Teams to generate and package client log information for troubleshooting. The resulting log package is saved locally, generally in the user's Downloads folder, where it can be attached to a support case or reviewed by the organization's support team. These logs provide useful client-side diagnostic data for investigating issues affecting Teams functionality, including meetings and screen sharing. Collecting the client logs is an appropriate first troubleshooting action because it captures evidence from the affected user's actual client session without requiring an administrator to alter Teams policies or configuration. Microsoft's Teams troubleshooting guidance specifically identifies this shortcut as the method for downloading desktop client logs on Windows. For the current collection steps and the log locations, see Use log files in troubleshooting Microsoft Teams and Collect Teams client logs.

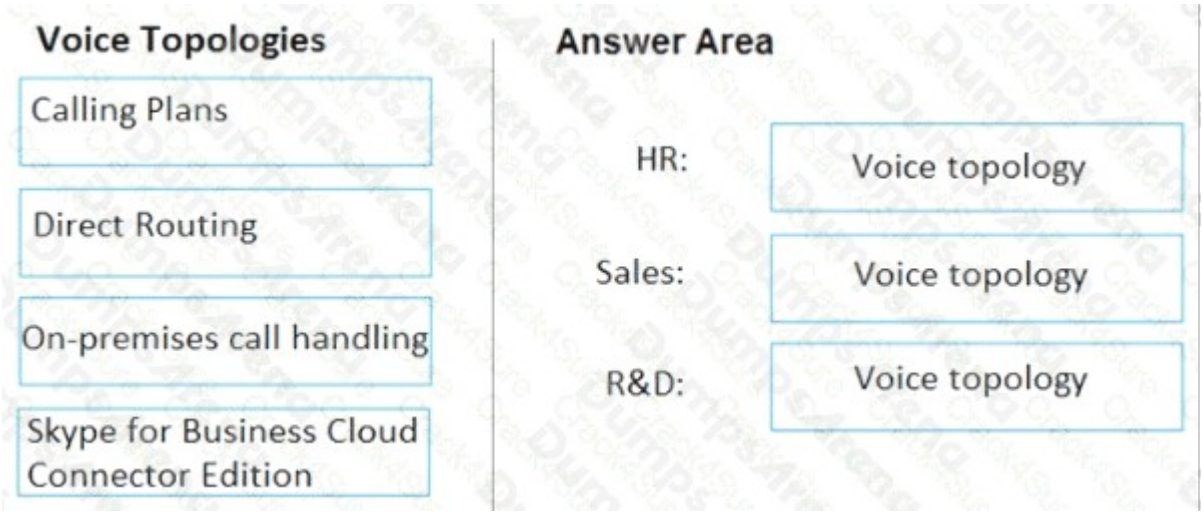
QUESTION NO: 35 - (DRAG DROP)

HOTSPOT

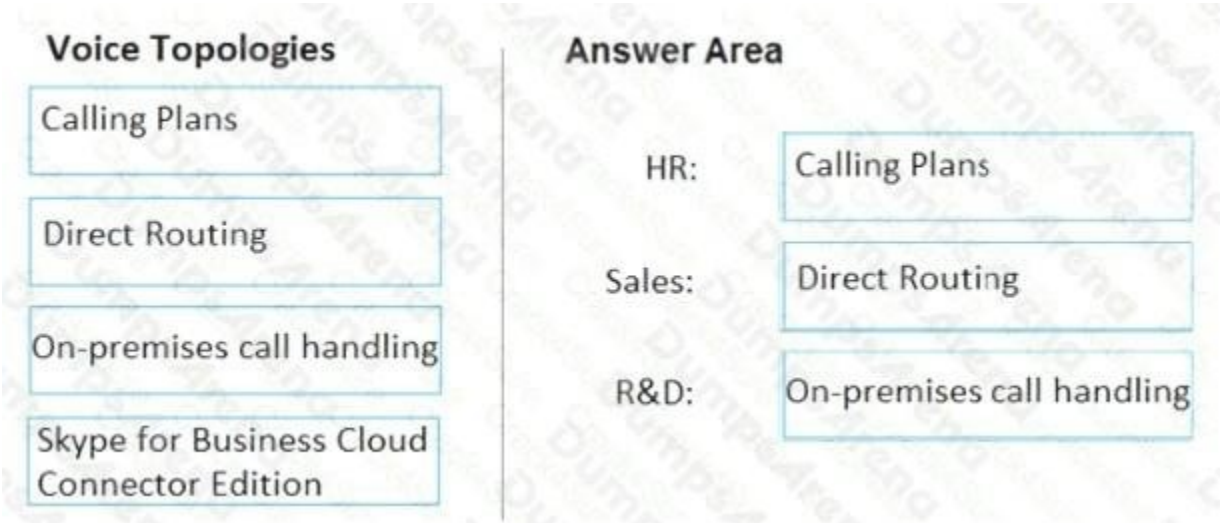
You need to recommend a voice topology for the departments. The topology must meet the calling requirements and the security requirements.

What should you recommend for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

The recommended topology assigns **Calling Plans** to HR, **Direct Routing** to Sales, and **On-premises call handling** to R&D. Calling Plans is the Microsoft-managed PSTN connectivity model for Teams Phone. It is appropriate where users need straightforward PSTN calling without the organization operating a Session Border Controller or managing a separate PSTN carrier connection. Microsoft provides the calling service and phone-number capabilities, which keeps deployment and operational overhead low. Microsoft's overview of this cloud-based PSTN option is available at Calling Plans for Teams.

Direct Routing is the appropriate recommendation for Sales because it connects Teams Phone to the PSTN through a certified Session Border Controller and the organization's selected carrier. This lets the organization retain control over PSTN routing, carrier arrangements, telephone-number management, and integrations with existing telephony infrastructure. It is a flexible model for departments that require a more customized voice deployment than a Microsoft-provided calling plan. Microsoft documents the architecture, certified SBC requirement, and configuration approach at Plan Direct Routing.

On-premises call handling is appropriate for R&D when the department's security requirement calls for voice call handling to remain within the organization's on-premises telephony environment. This topology supports a controlled hybrid voice design in which the organization preserves local handling for the calls subject to those security controls. Teams supports hybrid connectivity with Skype for Business Server for organizations that need to maintain applicable on-premises communications capabilities during their Teams deployment. Microsoft's guidance for planning hybrid connectivity is available at Plan hybrid connectivity between Teams and Skype for Business Server.

QUESTION NO: 36

You have a Microsoft 36S E5 subscription that uses Microsoft Teams.

You need to enforce multi-factor authentication (MFA) for all users that access Microsoft Teams outside the corporate network.

What should you configure?

A. a compliance policy

B. a Teams policy

C. a sign-in risk policy

D. a Conditional Access policy

ANSWER: D

Explanation:

A Conditional Access policy is the appropriate configuration because it can evaluate the context of each Microsoft Teams sign-in and require multifactor authentication when the access attempt originates outside the corporate network. In Microsoft Entra ID, define the corporate network as a named location, typically by specifying the organization's trusted public IP address ranges. Then create a Conditional Access policy that targets the required users and the Microsoft Teams cloud app, excludes the trusted named location, and uses the grant control to require multifactor authentication. This design lets users connecting from trusted corporate egress IP addresses sign in without the additional MFA challenge while enforcing MFA for access from all other locations. Conditional Access is designed to apply access controls based on signals such as user, application, device state, location, and sign-in risk. Microsoft recommends using Conditional Access policies to require MFA for cloud application access and to carefully exclude emergency access accounts from such policies to preserve administrative recovery access. For implementation guidance, see Require multifactor authentication for all users with Conditional Access and Conditional Access location conditions.

QUESTION NO: 37

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You company has a Microsoft 365 subscription and a Virtual Desktop Infrastructure (VDI) solution.

The company's Microsoft Teams upgrade policy is set to Teams only coexistence mode.

You deploy the Microsoft Installer (MSI) package for Microsoft Teams to the VDI solution.

Several months later, users of the VDI solution report that their workstation is missing several new Microsoft Teams features.

You need to ensure that the VDI solution users can use the new Microsoft Teams features.

Solution: You uninstall the Microsoft Teams MSI package, and then reinstall a new Microsoft Teams MSI package.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In a VDI deployment that uses the Teams MSI package, the Teams client version is managed through the virtual desktop image or the machine-level software deployment process. New Teams capabilities are delivered in newer client builds, so the VDI environment must receive an updated Teams installation to make those capabilities available to its users. Removing the existing MSI-installed client and installing a current Teams MSI package updates the client deployment and ensures that sessions launched from the refreshed VDI environment use the newer Teams build.

This approach is particularly appropriate for pooled and nonpersistent virtual desktops, where a user's changes are discarded at sign-out and client maintenance needs to be performed centrally. After the updated package is applied to the VDI image and that image is made available to the host pool, users receive the version containing the newer features when they connect. The Teams-only coexistence mode governs the organization's chat and calling experience; it does not eliminate the requirement to maintain an up-to-date Teams client in the VDI environment.

Microsoft documents Teams deployment and maintenance considerations for virtual desktops at Teams for Virtualized Desktop Infrastructure. For general information on how Teams client releases provide updates and features, see Teams client update process.

QUESTION NO: 38

Your company has a Microsoft 365 subscription that includes three groups: HR, Marketing, and Sales. You are tasked with configuring the Microsoft Teams desktop client to meet certain requirements. Which two actions should you take to ensure these requirements are fulfilled? Each correct answer contributes to part of the solution.

NOTE: Each correct selection is worth one point.

A. Modify the global app setup policy.

B. Modify the global app permission policy.

C. Create an app setup policy for HR.

D. Create an app setup policy for Marketing.

E. Create an app permission policy for Marketing.

F. Create an app permission policy for HR.

ANSWER: C D

Explanation:

Create an app setup policy for HR and create an app setup policy for Marketing to provide department-specific Teams desktop client configurations. An app setup policy controls the apps that Teams installs for users and, importantly, the apps pinned to the Teams app bar and their ordering. This makes it the appropriate policy type when separate user populations need different default app experiences in Teams.

Creating distinct policies allows the HR and Marketing populations to receive their respective configured app layouts without applying the same configuration to every user in the tenant. After configuring the policies, the administrator assigns each one to the appropriate users or Microsoft 365 group through Teams policy assignment. This supports targeted administration while maintaining an independent default experience for other users, including Sales. Microsoft documents app setup policies as the mechanism for managing installed and pinned apps in the Teams client, including app bar pinning and order. Teams policy assignment also supports applying appropriate policies to user groups. See Manage app setup policies in Microsoft Teams and Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 39

Your organization subscribes to Microsoft 365, and all employees have been given a Microsoft 365 E3 license.

You are tasked with implementing information barriers between two specific groups of users within the company.

Identify the two licensing add-ons that enable this functionality. Each correct selection represents a full solution.

Note: Each correct selection is worth one point.

A. Microsoft Defender for Office 365

B. Insider Risk Management

C. Compliance

D. Communications Credits

ANSWER: B C

Explanation:

Information barriers are a Microsoft Purview feature that prevents communication and collaboration between users assigned to conflicting segments. They can be used to control interactions in Microsoft Teams, including chats, calls, meetings, team membership, and user discovery, as well as supporting information-barrier controls across other Microsoft 365 services. Microsoft 365 E3 by itself does not provide the required entitlement for this capability. Organizations can retain Microsoft 365 E3 as the foundational license and assign an eligible compliance add-on to the users who must be covered by information barrier policies. **Insider Risk Management** is correct because the Microsoft 365 E5 Insider Risk Management add-on is listed as an eligible license for Microsoft Purview Information Barriers. **Compliance** is also correct because the Microsoft 365 E5 Compliance add-on includes the entitlement needed for Information Barriers. Licensing must cover the users participating in the policy, rather than only the administrator who creates it. After licensing is in place, administrators define segments and create policies that block the prohibited communications between them. Microsoft documents the eligible licensing and policy prerequisites at Microsoft Purview Information Barriers and describes the Teams behavior at Information barriers in Microsoft Teams.

QUESTION NO: 40

You have a Microsoft 365 subscription that integrates Microsoft Teams for your organization. You need to identify which Teams were inactive over the last 90 days. What tool or report should you use to accomplish this task?

A. Teams advisor

B. the Office 365 Groups activity report

C. the Teams user activity report

D. the Teams usage report

ANSWER: B

Explanation:

The Office 365 Groups activity report is the appropriate report because every Microsoft Team is associated with a Microsoft 365 group. This report provides group-level activity information that can be used to assess whether the group behind a Team has been active during a selected reporting period, including 90 days. Its detailed view and downloadable data include identifiers such as the group display name and last activity date, together with workload activity measures. An administrator can select the 90-day reporting period, review the last activity information, and identify Teams whose associated Microsoft 365 groups show no activity in that period. This makes the report useful for Teams governance and lifecycle tasks, such as reviewing potentially unused Teams before taking action under the organization's retention, expiration, or archival processes. Microsoft documents that the Microsoft 365 Groups activity report shows activity across services associated with Microsoft 365 groups, including Teams, and supports reporting-period analysis. For the report fields and available periods, see Microsoft 365 Groups activity report. For general administration of usage reporting in the Microsoft 365 admin center, see Microsoft 365 admin center activity reports.

QUESTION NO: 41

You have a Microsoft 365 subscription with Microsoft Teams implemented.

You are planning to deploy Microsoft Teams voice capabilities.

Which two settings require a resource account? Each correct answer is a part of the solution.

Note: Each correct selection is worth one point.

A. Call park policies

B. Auto attendant

C. Call queues

D. Emergency polices

E. Guest access

ANSWER: B C

Explanation:

Auto attendant and Call queues require Teams resource accounts. A resource account is a Microsoft Entra ID account that represents a voice application rather than an individual user. It provides the identity used to associate an auto attendant or call queue with Teams and, when the service must receive calls from the public switched telephone network, it can be assigned a telephone number. For an auto attendant, the resource account identifies the automated call-answering service that presents greetings, menus, and routing choices to callers. For a call queue, it identifies the queue endpoint that accepts incoming calls and distributes them to the configured agents according to the queue settings. Organizations can use resource accounts with a Teams Phone Resource Account license where no phone number is required, or assign suitable licensing and a number when callers must dial the application directly. Microsoft states that resource accounts are required for auto attendants and call queues, and admins associate each resource account with the relevant voice application during configuration. See Manage resource accounts in Teams and Plan for Teams auto attendants and call queues.

QUESTION NO: 42 - (DRAG DROP)

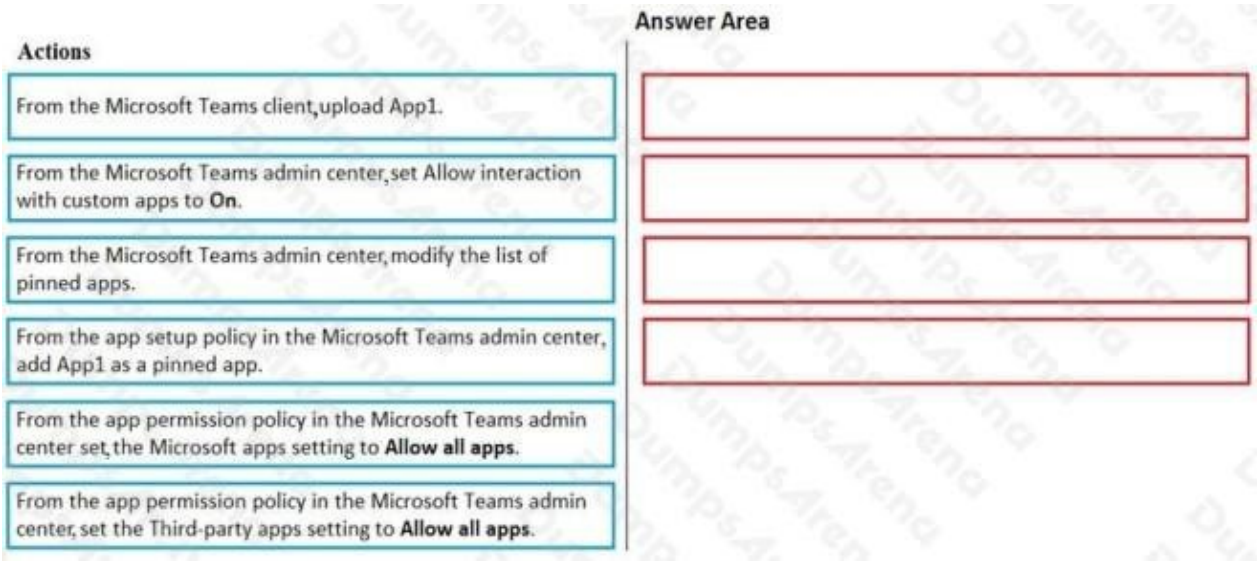
DRAG DROP

Your company has a custom Microsoft Teams app named App1.

You need to deploy App1. The solution must ensure that App1 appears as the first item on the app bar of the Microsoft Teams client.

Which four actions should you perform in sequence? To answer, move the actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



ANSWER:



Explanation:

The required sequence begins by setting **Allow interaction with custom apps** to **On** in the Microsoft Teams admin center. This is the tenant-level prerequisite that allows users to interact with custom Teams apps and supports the organization's use of its internally developed app. With custom-app interaction enabled, App1 can then be uploaded from the Microsoft Teams client so that the app package is available in the tenant for deployment. Microsoft describes the tenant settings and controls for custom apps in its custom app policies and settings documentation.

After the app has been uploaded, the administrator uses an app setup policy to add App1 as a pinned app. App setup policies are the Teams policy mechanism that controls which apps are installed and pinned for users. Assigning the applicable policy causes the pinned app configuration to be delivered to the users covered by that policy. This is the appropriate policy type because the requirement concerns the Teams client app bar rather than merely whether the app is permitted for use. Microsoft documents installing and pinning apps through these policies in Manage app setup policies in Microsoft Teams.

Finally, the pinned-app list must be modified to place App1 at the top. The order configured in the policy's pinned-app list determines the order in which pinned apps appear in the Teams client app bar. Moving App1 to the first position therefore satisfies the requirement that it appear as the first app-bar item for users who receive the policy. This sequence enables the

custom app, makes it available, applies the pinning configuration, and then explicitly establishes the required display position.

QUESTION NO: 43

Your organization uses Microsoft Teams and Microsoft Purview.

You need to prevent users from sending messages that contain credit card numbers in Teams chats and channel messages.

Which two actions should you take when creating the data loss prevention (DLP) policy? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. Select Teams chat and channel messages as a policy location.

B. Configure a rule that detects the Credit Card Number sensitive information type.

C. Configure the rule to block or restrict matching messages.

D. Select Exchange email as the only policy location.

E. Create a retention label for the Teams channel.

ANSWER: A B C

Explanation:

Select **Teams chat and channel messages** as a location for the DLP policy. This location enables Microsoft Purview DLP to evaluate Teams messages. A policy scoped only to Exchange, SharePoint, or OneDrive would not evaluate the text of Teams chat and channel messages.

Configure a rule that detects the appropriate sensitive information type, such as Credit Card Number, and configure the rule to block or restrict the message. DLP uses sensitive information types and associated detection logic to identify regulated data. The rule action can prevent the message from being sent and can notify the sender according to the configured policy behavior.

Teams DLP for messages does not govern the retention of messages or files. Microsoft documents Teams message protection in Learn about data loss prevention for Microsoft Teams.

QUESTION NO: 44

You have an active subscription to Microsoft Office 365.

Your task is to ensure that guest users are unable to delete any channels from a Microsoft Teams team.

Which tool or method should you use to achieve this?

A. the Microsoft 365 admin center

B. the Microsoft Teams PowerShell module

C. the Azure Active Directory admin center

D. the Security & Compliance admin center

ANSWER: B

Explanation:

The Microsoft Teams PowerShell module is the appropriate administrative method because guest channel-deletion permission is a configurable property of an individual Microsoft Teams team. An administrator can connect to the Teams PowerShell service and use the `Set-Team` cmdlet to update the target team's guest capabilities. Specifically, setting `AllowGuestDeleteChannels` to `$false` prevents guest members from deleting standard channels in that team. For example, an administrator can run `Set-Team -GroupId <group-id> -AllowGuestDeleteChannels $false`, using the Microsoft 365 group ID associated with the team. This is useful when an organization wants to permit guest collaboration while retaining control of the team's channel structure. The setting applies at the team level, so it can be configured according to the governance needs of each team rather than requiring the same choice for every team in the tenant. The `Set-Team` cmdlet documentation lists guest channel permissions, including the parameter used to control whether guests can delete channels. For implementation details and supported parameters, see Set-Team documentation and the Microsoft Teams PowerShell overview.

QUESTION NO: 45

Your organization has an active Microsoft 365 subscription.

You need to ensure that only the users within the research department of your company are restricted from deleting chat messages.

Which initial step should you take within the Microsoft Teams admin center?

A. Configure the Meeting settings.

B. Create a new messaging policy.

C. Modify the global messaging policy.

D. Create a new meeting policy.

ANSWER: B

Explanation:

Create a new messaging policy. Teams messaging policies control the chat and channel messaging capabilities available to users, including the ability to delete sent chat messages. To limit this restriction to the research department, an administrator should first create a custom messaging policy in the Teams admin center. In that policy, disable the setting that permits users to delete their sent messages. The policy can then be assigned to the relevant research users, either individually or through a group-based policy assignment when the department is represented by an appropriate Microsoft Entra group. This targeted policy approach applies the required control only to the intended department while retaining the existing messaging permissions for everyone else. Microsoft documents the available controls in Teams messaging policies, including deletion of sent messages, at Messaging policies in Microsoft Teams. For details on assigning a custom policy to users or groups, see Assign policies to users and groups in Teams.

QUESTION NO: 46

As a Systems Administrator for your company, which has recently obtained a Microsoft 365 subscription, you are responsible for configuring Microsoft Teams. All employees have been granted a Microsoft 365 E3 license.

According to your company's security policy, users are prohibited from adding apps to Microsoft Teams.

Which configuration should you apply to Microsoft Teams to fulfill this security requirement?

A. The global app permission policy.

B. The global Teams policy.

C. The Org-wide Teams settings.

D. The global app setup policy.

ANSWER: A

Explanation:

The global app permission policy is the appropriate configuration because Teams app permission policies control the apps that users are permitted to access, install, and use. Applying the Global (Org-wide default) policy affects users throughout the organization unless a more specific policy is assigned. To enforce a company-wide requirement that employees cannot add apps, the administrator can configure this policy to block the relevant app categories and individual apps, preventing those apps from being available for installation or use in Teams.

App permission policies provide the access-control layer for Teams apps, including Microsoft-provided, third-party, and custom apps. This makes the policy suitable for implementing an organization's security decision about app availability, rather than simply determining which approved apps appear in the Teams client. Microsoft documents that app permission policies let administrators control which apps are available to users, while the organization-wide default policy is the baseline applied across the tenant. See Manage app permission policies in Microsoft Teams and Manage Teams apps.

QUESTION NO: 47

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has a Microsoft 365 subscription.

You plan to configure the environment to allow external users to collaborate in Microsoft Teams by using guest access.

The company implements a new security policy that has the following requirements:

Requirement details were not provided in the original text.

You need to recommend a solution to meet the security policy requirements.

Solution: You propose running the `New-CSExternalAccessPolicy` and `Set-CSExternalAccessPolicy` cmdlets using PowerShell.

Does this solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. `New-CsExternalAccessPolicy` and `Set-CsExternalAccessPolicy` manage Teams external access (federation) policies. External access lets tenant users find, chat, call, and meet with people in other Teams organizations without making those people guests in the company's tenant. It is therefore a separate collaboration model from guest access and does not configure the guest-access controls required to admit external users into teams and channels.

Teams guest access relies on Microsoft Entra B2B collaboration and the Teams guest-access configuration. An administrator must enable guest access in Teams and ensure that the associated Microsoft 365 Groups, SharePoint, OneDrive, and Microsoft Entra external-collaboration settings permit the intended guest experience. Teams policies can then control capabilities available to guests after they are added. Because the proposed cmdlets address federation rather than tenant guest membership and guest permissions, they do not meet a goal to configure collaboration by using guest access. Microsoft distinguishes these models in its Teams guest access documentation and documents external-access policy management separately in the New-CsExternalAccessPolicy PowerShell reference.

QUESTION NO: 48

Your company has 200 employees.

You are planning to transition all users from Skype for Business Online to Microsoft Teams, ensuring that Enterprise Voice is enabled for everyone.

Which coexistence mode should you suggest within the Microsoft Teams upgrade policy for a smooth transition?

A. Skype for Business with Teams collaboration

B. Islands

C. Teams only

D. Skype for Business with Teams collaboration and meetings

ANSWER: D

Explanation:

Skype for Business with Teams collaboration and meetings is the appropriate transitional coexistence mode for a meetings-first migration. It moves users' collaboration and meeting experiences to Teams, allowing the organization to introduce Teams meetings, channels, and associated user-adoption processes while retaining Skype for Business for chat and calling during the transition. This is particularly useful where Enterprise Voice must remain available without interruption, because existing voice calling can continue to be handled through Skype for Business while Teams readiness is completed.

The organization can use this period to validate calling devices, complete number and voice-routing migration work, communicate the new meeting experience, and ensure that all users have the required Teams calling configuration before completing the upgrade. When those voice migration prerequisites are complete, users can be moved to Teams-only mode, where Teams becomes the client for chat, meetings, and calling. Microsoft identifies this policy mode as one that directs meetings to Teams while Skype for Business continues to provide chat and calling functionality during coexistence. See Teams and Skype for Business coexistence and interoperability and Configure coexistence and upgrade settings.

QUESTION NO: 49

You have a Microsoft 365 subscription that includes Microsoft Teams, and all users presently have the Microsoft Office 365 Enterprise E3 license. You need to ensure that users can join scheduled meetings by dialing in to a toll-free phone number. Which two add-on licenses should you assign to the users to achieve this functionality? Each correct answer is worth one point.

A. Communication Credits

B. Microsoft 365 Phone System - Virtual User

C. Microsoft 365 Domestic Calling Plan

D. Microsoft 365 Audio Conferencing

E. Common Area Phone

ANSWER: A D

Explanation:

Microsoft 365 Audio Conferencing provides the meeting dial-in capability required for Teams meetings. When it is assigned to a meeting organizer, Teams can include audio-conferencing details in scheduled meeting invitations, enabling attendees to join the meeting audio over the public telephone network rather than through the Teams client. This feature is designed for participants who need telephone access to a meeting, including attendees who cannot use an internet connection or Teams application at the time of the meeting.

Communication Credits supply the tenant-level prepaid funding needed for chargeable audio-conferencing services, including toll-free dial-in usage. A toll-free number shifts call costs from the attendee to the organization; therefore, the organization must have Communication Credits configured to cover the associated minutes. Administrators acquire and configure the credits for the tenant and can set an automatic recharge amount and threshold so toll-free access remains

available as the balance is consumed. Together, Audio Conferencing enables the dial-in meeting experience and Communication Credits fund usage of the toll-free number. See Set up Audio Conferencing for Microsoft Teams and What are Communications Credits?.

QUESTION NO: 50 - (HOTSPOT)

You have a Microsoft 365 subscription.

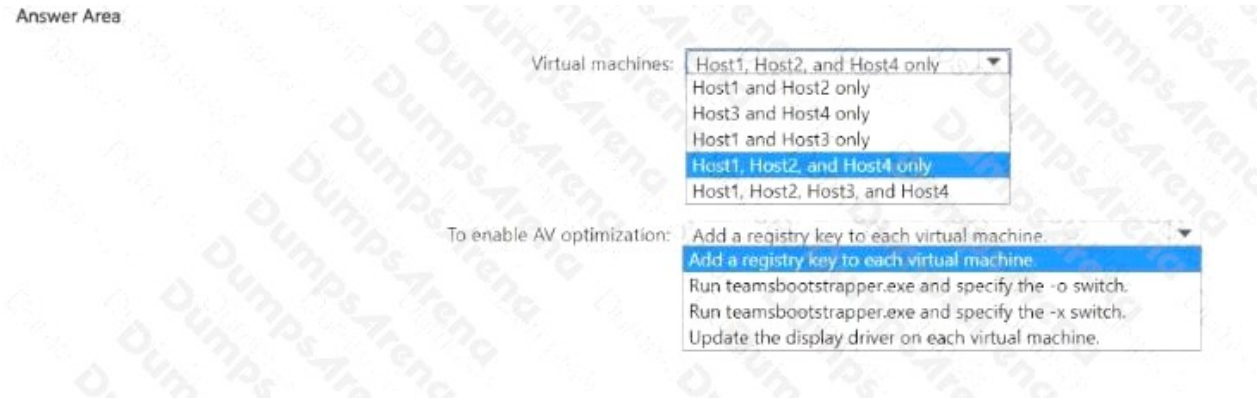
You have a virtualized desktop infrastructure (VDI) that contains the virtual machines shown in the following table.

Name	Operating system	VDI platform
Host1	Windows 10	Azure Virtual Desktop
Host2	Windows 11	Amazon WorkSpaces
Host3	Windows Server 2019	Citrix Virtual Apps and Desktops
Host4	Windows Server 2016	VMware Horizon

You need to install the Teams for VDI client on the virtual machines. The solution must support audio/video (AV) optimization.

Which virtual machines support the Teams for VDI client, and what should you do to enable AV optimization? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

Teams in a virtual desktop infrastructure needs a supported VDI provider and a supported Windows session-host operating system so that its media engine can redirect audio and video processing to the user's local endpoint. In this environment, the qualifying session hosts are Host1, which uses Windows 10 with Azure Virtual Desktop; Host3, which uses Windows Server 2019 with Citrix Virtual Apps and Desktops; and Host4, which uses Windows Server 2016 with VMware Horizon. These are the virtual machines on which the Teams for VDI client can be used with the intended optimized media architecture.

To turn on the optimization behavior, configure the Teams VDI registry setting on every applicable virtual machine. This setting identifies the session host as a virtualized Teams environment and lets Teams use the VDI media-redirection path rather than processing the full real-time audio and video workload inside the virtual machine. This is important because optimized media keeps latency, CPU use, bandwidth consumption, and user experience under control by handling the media as close to the endpoint as possible. Microsoft's Teams VDI guidance describes the supported architecture and the use of media optimization for virtual desktop deployments: Teams for Virtualized Desktop Infrastructure. Microsoft also documents the Azure Virtual Desktop media optimization design in Use Microsoft Teams on Azure Virtual Desktop.

QUESTION NO: 51

As a Systems Administrator, you have configured Microsoft 365 for your organization, where all users possess a Microsoft 365 E5 license. Each company department has its own private team, and there is an additional team named Managers for all departmental leaders. You want to prevent the Managers team from appearing in the Suggested Teams list. How can this be achieved?

A. Modify the member permissions for the Managers team.

B. Configure a new app permission policy.

C. Modify the Team discovery options for the Managers team.

D. Select the Hide option for the Managers team.

ANSWER: C

Explanation:

Modify the Team discovery options for the Managers team. Microsoft Teams supports discovery settings for private teams that control whether people who are not already members can find those teams through Teams discovery experiences, including search and suggestions. For a leadership-only private team, turning off its discoverability prevents the team from being promoted to other users as a suggested team while allowing its existing owners and members to continue using it normally. This is the appropriate control because it governs the team's visibility to nonmembers rather than changing the team's membership or its collaboration settings. An administrator can manage private-team discoverability in the Teams admin center, and team owners can manage the applicable discovery setting when their organization permits it. The setting is designed for cases where a team must remain private and accessible only through direct membership, such as a Managers team containing leadership discussions or confidential business information. Microsoft's guidance describes how to manage whether private teams are discoverable and how that visibility affects users who are not members. See Manage discovery of private teams in Microsoft Teams and Private teams in Microsoft Teams.

QUESTION NO: 52

Your company has a Microsoft 365 subscription.

You need to ensure that users from a partner company named Contoso, Ltd. can collaborate with your

company ' s users in teams. The solution must ensure that the Contoso users can exchange chat messages in channels.

Which three actions should you perform before you add the Contoso users to teams? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group members outside the organization access group content to **On** .

B. From the Guest access settings in the Microsoft Teams admin center, set Allow guest access in Microsoft Teams to **On** .

C. From the External collaboration settings in the Azure Active Directory admin center, add Contoso ' s domain to the list of target domains.

D. From the External access settings in the Microsoft Teams admin center, add Contoso ' s domain to theAllowed list of domains.

E. From the External collaboration settings in the Azure Active Directory admin center, set Guest userspermissions are limited to **No** .

F. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group owners add people outside the organization to groups to **On** .

ANSWER: A B F

Explanation:

Contoso users must be configured as guests because channel conversations are team content and guest members can participate in channel posts and replies. Enabling guest access in the Microsoft Teams admin center activates the Teams guest experience for the tenant, allowing invited external users to take part in teams according to the configured guest capabilities. Teams uses Microsoft 365 groups for team membership, so the Microsoft 365 Groups guest settings must also permit group owners to add people from outside the organization. This allows a team owner to invite and add the Contoso users as guest members. Finally, guest users must be allowed to access group content. That setting grants the guests access to the underlying Microsoft 365 group resources that support the team, including the content and conversations available through their team membership. Together, these settings establish the required guest invitation, membership, and access path before the Contoso users are added to a team. Microsoft documents the Teams guest-access requirements and describes the Microsoft 365 Groups guest settings that Teams depends on. See Guest access in Microsoft Teams and Guest access in Microsoft 365 Groups.

QUESTION NO: 53

You have a Microsoft 365 E5 subscription that includes Teams. You need to ensure that all files stored in Teams channels are retained for at least one year after deletion. What action should you take?

A. Create an Audit retention policy.

B. Enable Customer Lockbox.

C. Create a data loss prevention (DIP) policy for Teams chat and channel messages.

D. Create a retention policy for Microsoft SharePoint sites.

ANSWER: D

Explanation:

Create a retention policy for Microsoft SharePoint sites. Files uploaded to Teams channels are stored in SharePoint rather than in the Teams messaging service. A standard channel uses the document library in the SharePoint site connected to its team. Private and shared channels use separate SharePoint sites, so the retention configuration must cover the applicable SharePoint sites to protect files in all relevant channel types. In Microsoft Purview, configure a retention policy for the SharePoint location, include the required team-connected and channel sites, and set the retention period to at least one year. When the policy is configured to retain content, SharePoint preserves retained files for the policy duration even after a user deletes them. This supports compliance retention requirements and ensures the content can remain discoverable through the appropriate compliance processes during its retention period. Teams message retention and Teams file retention are configured through different workloads: Teams policies govern chat and channel messages, while SharePoint retention governs channel files. For configuration guidance, see Learn about retention for Microsoft Teams and Create and configure retention policies.

QUESTION NO: 54 - (SIMULATION)

You have a Microsoft 365 subscription that uses Teams.

You have a meeting room that contains a Teams Rooms device and a Surface Hub.

You have the following configuration file for the Teams Rooms device.

For each of the following statements, select Yes if True. Otherwise select No. NOTE: Each correct selection is worth one point.

ANSWER: See the explanation for the answer

Explanation:

Cannot determine the Yes/No selections because the configuration file and the statements to evaluate are not included in the supplied question JSON.

Please provide the Teams Rooms configuration file (for example, the `SkypeSettings.xml` contents or screenshot) and each statement.

QUESTION NO: 55

Your company operates five distinct office locations, each with its own unique phone number. You are planning to implement a Phone System across all offices. To optimize administration efforts, you need to ensure that every office has its own unique greeting message for weekdays and a separate unique message for weekends. What should you create to achieve this?

A. one auto attendant that contains all five phone numbers

B. one call queue that contains all five phone numbers

C. five auto attendants that each contains one phone number

D. five call queues that each contains one phone number

ANSWER: C

Explanation:

five auto attendants that each contains one phone number is correct. A Teams auto attendant is the call-handling service used to answer calls to an organizational number, play a greeting, and direct callers according to a configured call flow. Each auto attendant has its own business-hours schedule and after-hours handling. For each office, the weekday operating schedule can be configured as business hours and the weekend can be handled through the after-hours schedule. This allows the administrator to define a location-specific greeting for callers during weekdays and another location-specific greeting for callers during weekends.

Creating a separate auto attendant for each office also provides a clear administrative boundary for that office's call flow. Each auto attendant can be associated with a dedicated resource account, and the resource account can be assigned the office's individual telephone number. As a result, calls to each of the five published numbers reach the corresponding auto attendant and receive the greetings appropriate to that location and time of week. This design supports independent updates to schedules, greetings, and routing as office requirements change. Microsoft describes auto attendants, their business-hours and after-hours call handling, and resource-account number assignment in its Teams auto attendant configuration guidance and resource account management guidance.

QUESTION NO: 56 - (HOTSPOT)

Your company uses Microsoft Teams.

You have a meeting policy named Policy1 that is assigned to a group named Sales.

You need to ensure that all the meetings recorded by the Sales group are stored indefinitely.

How should you complete the PowerShell cmdlet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

To retain recordings made by users governed by Policy1 indefinitely, update the existing Teams meeting policy with `Set-CsTeamsMeetingPolicy`. This cmdlet is designed to modify settings on a Teams meeting policy, and specifying `-Identity Policy1` ensures that the change is made to the policy assigned to the Sales group.

The relevant retention control is `-NewMeetingRecordingExpirationDays`. This setting defines the expiration period for newly created Teams meeting recordings associated with the policy. Using a value of `-1` disables the expiration period, so new recordings do not automatically expire. As a result, recordings created by Sales users while Policy1 applies are retained indefinitely, unless they are manually deleted or affected by a separate retention or compliance policy.

The completed command is `Set-CsTeamsMeetingPolicy -Identity Policy1 -NewMeetingRecordingExpirationDays -1`. Microsoft documents the `NewMeetingRecordingExpirationDays` setting in the Teams meeting policy PowerShell reference and notes that a value of `-1` means recordings never expire. See the Set-CsTeamsMeetingPolicy documentation and Microsoft's guidance on meeting recording expiration.

QUESTION NO: 57 - (SIMULATION)

Task 9

You need to deploy the Microsoft Viva Connections app to Teams and install the app as the first item on the app bar of the Teams client for all users.

ANSWER: See the explanation for the answer

Explanation:

In the Microsoft Teams admin center, configure the organization-wide app setup policy:

1. Go to `Teams apps` > `Setup policies`.
2. Open `Global (Org-wide default)` (or the setup policy assigned to all target users).
3. Under **Installed apps**, select `Add apps`, find and add `Viva Connections`.
4. Under **Pinned apps**, select `Add apps`, find and add `Viva Connections`.
5. Move `Viva Connections` to the top/first position in the pinned-app list.
6. Select `Save`.

This deploys Viva Connections to users and pins it as the first item on the Teams client app bar.

Manage app setup policies in Microsoft Teams

QUESTION NO: 58

Your organization holds a Microsoft 365 subscription. A user known as User5 is unable to initiate calls using Microsoft Teams. Upon inspecting the Microsoft Teams client for User5, you notice that the dial pad is missing. However, other employees within the company experience no difficulty in making calls. What two steps should you take to resolve this issue and enable User5 to make calls successfully? Each correct step is a part of the solution.

NOTE: Selecting each correct option earns you one point.

A. Modify the caller ID properties of User5.

B. Assign a Phone System license to User5.

C. Assign a SIP address to User5.

D. Assign an app setup policy to User5.

E. Enable User5 for Enterprise Voice.

ANSWER: B E

Explanation:

Assign a Phone System license to User5 and enable User5 for Enterprise Voice. Teams Phone, previously named Phone System, is the Microsoft 365 service that provides private branch exchange capabilities for Teams, including PSTN calling functionality. The user must have the applicable Teams Phone service entitlement so that Teams can provision calling capabilities for that specific account. Licensing is evaluated per user; therefore, the fact that other employees can place calls does not provide the required calling entitlement to User5.

Enterprise Voice must also be enabled for the user. This establishes that the account is enabled for enterprise voice functionality and can use the organization's configured PSTN connectivity and voice-routing configuration. In modern Teams administration, this status can be set while assigning a phone number by using the `EnterpriseVoiceEnabled` parameter of `Set-CsPhoneNumberAssignment`. Once the appropriate Teams Phone license is assigned and enterprise voice is enabled, Teams can provision User5's outbound PSTN-calling experience, including the dial pad. Microsoft describes Teams Phone and its licensing requirements in the Teams add-on licensing documentation and documents Enterprise Voice configuration in the Set-CsPhoneNumberAssignment reference.

QUESTION NO: 59

Your company has a Microsoft 365 subscription.

You need to ensure that only the members of the company ' s IT group can create private channels.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Modify the global teams policy.

B. Assign the members of the IT group to the policy.

C. Create a custom teams policy.

D. Run the Sec-TeamsChannel cmdlet.

E. Modify the global messaging policy.

F. Create a custom messaging policy.

ANSWER: A B C

Explanation:

Private-channel creation is governed by a Teams channels policy, specifically the policy setting that controls whether users can create private channels. To limit this capability to the IT group, first modify the global teams policy so private-channel creation is disabled for the default population. Because the global policy applies to users who do not receive a more-specific assigned policy, this establishes the required organization-wide restriction.

Next, create a custom teams policy that enables private-channel creation. A custom policy provides an exception to the global restriction without changing the baseline configuration for everyone else. Finally, assign the members of the IT group to the policy. The assigned custom policy takes precedence for those users, allowing them to create private channels while users who remain under the global policy cannot do so. Policy assignments can be made to individual users or managed

through supported group-based policy assignment where appropriate. Microsoft documents Teams channel policies and their private-channel creation control at Teams policies and describes private-channel administration at Private channels in Microsoft Teams.

QUESTION NO: 60

Your organization's network includes an on-premises Active Directory domain integrated with a Microsoft 365 subscription. You have created a new team named Sales using the Microsoft Teams client, and you need to ensure all individuals within your company's sales department are included as members of the team. The process should automatically add any new employees who join the sales department to the team. Which tool would you use to set up the membership configurations for the Sales group?

A. Active Directory Users and Computers

B. the Microsoft 365 admin center

C. Azure AD Connect

D. the Azure Active Directory admin center

ANSWER: D

Explanation:

the Azure Active Directory admin center is correct because every team is backed by a Microsoft 365 group, and the group's membership can be managed through Microsoft Entra ID, formerly named Azure Active Directory. To make the Sales team include everyone whose department is Sales, an administrator configures the associated Microsoft 365 group with *Dynamic User* membership and creates a membership rule based on the user department attribute, such as `user.department -eq "Sales"`.

Microsoft Entra ID continuously evaluates the rule against directory user attributes. Therefore, when a new employee is synchronized from the on-premises Active Directory environment and has their department populated as Sales, the user is automatically added to the Microsoft 365 group. Because that group provides the membership for the connected Teams team, the employee then receives membership in the Sales team without a manual invitation. Dynamic group membership requires appropriate Microsoft Entra ID licensing for the users evaluated by the rule. Microsoft documents the Teams relationship with dynamic Microsoft 365 groups and the available dynamic membership-rule configuration in Dynamic membership for Teams and Dynamic membership rules for groups.

QUESTION NO: 61

Your company deploys a Quality of Service (QoS) solution to its network.

You recently deployed Microsoft Teams for all users. Each user uses a domain-joined computer that runs Windows 10.

The users report poor audio quality when they use Microsoft Teams from the network.

You discover that the media traffic from Microsoft Teams is **NOT** processed by the QoS solution.

You need to ensure that all the media traffic is processed by the QoS solution.

Which two actions should you perform? Each correct solution presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Microsoft Teams client, select a certified Microsoft Teams audio device.

B. From PowerShell, run the Set-CsQoEConfiguration cmdlet.

C. From Group Policy Management, create a Group Policy Object (GPO) that contains the Policy based QoS settings, and then link the GPO to the domain.

D. From the Microsoft Teams admin center, turn on logging for the device configuration profile.

E. From the Microsoft Teams admin center, configure client media port ranges that match the port ranges in the Policy-based QoS GPO.

ANSWER: C E

Explanation:

For Windows domain-joined endpoints, Policy-based QoS delivered through Group Policy is the appropriate mechanism for classifying Teams media and applying the DSCP markings expected by the organization's network QoS infrastructure. The Group Policy Object should define the Teams media traffic criteria, including the relevant executable, protocol, source-port range, and DSCP value, and be linked where the affected computer accounts receive it. This ensures that marking occurs at the client endpoint before traffic enters the network.

The Teams client media port ranges must also be explicitly configured in the Teams admin center so that Teams uses predictable, non-overlapping ports for audio, video, and application sharing. Those ranges must correspond to the source-port ranges defined in the Policy-based QoS policy. Aligning the Teams-assigned media ports with the GPO classification criteria lets the policy consistently identify every type of real-time Teams media flow and submit it to the QoS treatment configured on network devices. Microsoft documents both endpoint QoS configuration and the need to coordinate Teams media port ranges with QoS policies. See Quality of Service in Microsoft Teams and Manage meeting settings in Microsoft Teams.

QUESTION NO: 62

You have a Microsoft 365 subscription with Microsoft Teams in use.

Your goal is to ensure that only specific applications are available in the Microsoft Teams app store while minimizing administrative tasks.

Which action should you take to achieve this?

A. Configure the Org-wide app settings

B. From the Manage apps page, block unapproved apps

C. Configure the global (Org-wide default) app permission policy

D. Configure the global (Org-wide default) app setup policy

ANSWER: C

Explanation:

Configure the global (Org-wide default) app permission policy. Teams app permission policies determine which Microsoft, third-party, and custom apps are available to users in Teams. An administrator can configure the global policy to permit only selected apps and block all other apps in the applicable app categories. This provides centralized control over the apps users can find and use without requiring an administrator to configure or assign individual policies for every user.

The global (Org-wide default) policy is applied to all users unless a more specific app permission policy is assigned. Therefore, it is the most efficient choice when the same restricted app catalog should apply across the organization. If a limited set of users later requires different app access, separate policies can be created and assigned only to those exceptions, while the global policy continues to govern everyone else. This approach implements an allow-list model and minimizes ongoing administrative work because the organization-wide baseline is managed in one policy. Microsoft describes how app permission policies control user access to Teams apps in Manage app permission policies in Microsoft Teams. For broader app governance and management in the Teams admin center, see Manage apps in the Teams admin center.

QUESTION NO: 63

Your organization has a Microsoft 365 subscription. You need to enable users from a partner organization named Contoso, Ltd. to collaborate with your company's users in Microsoft Teams. The solution must ensure that Contoso users can engage in chat conversations within channels.

Which three actions should you take prior to adding the Contoso users to Teams? Each correct choice constitutes a portion of the solution.

NOTE: Each correct selection is worth one point.

A. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group members outside the organization access group content to On.

B. From the Guest access settings in the Microsoft Teams admin center, set Allow guest access in Microsoft Teams to On.

C. From the External collaboration settings in the Azure Active Directory admin center, add Contoso's domain to the list of target domains.

D. From the External access settings in the Microsoft Teams admin center, add Contoso's domain to the Allowed list of domains.

E. From the External collaboration settings in the Azure Active Directory admin center, set Guest users permissions are limited to No.

F. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group owners add people outside the organization to groups to On.

ANSWER: A B F

Explanation:

Channel conversations are part of the team experience, so Contoso users must be configured as Microsoft Teams guests rather than merely as external chat contacts. Setting **Allow guest access in Microsoft Teams** to On enables the Teams guest experience and permits guests to participate in the team capabilities available under the tenant's guest-access policy, including channel conversations.

Teams are backed by Microsoft 365 groups. Therefore, the group configuration must permit the organization to invite external people and permit those invited people to use the group's content. Setting **Let group owners add people outside the organization to groups** to On allows a team owner to add a Contoso user as a guest. Setting **Let group members outside the organization access group content** to On allows the guest to access the resources and conversations associated with the group-backed team. Together, these settings establish the required tenant-level prerequisites before the users are added to the team. Microsoft describes the Teams guest-access requirements at Guest access in Microsoft Teams and the Microsoft 365 group guest controls at Collaborate with guests in a team.

QUESTION NO: 64

Your organization wants to deploy the Walkie Talkie app in Microsoft Teams to a group of frontline workers.

You need to ensure that the users can use the app and that the app appears in their Teams app bar.

Which two actions should you take? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. Configure an app permission policy that allows the Walkie Talkie app.

B. Configure an app setup policy that installs and pins the Walkie Talkie app.

C. Create a Teams meeting policy that enables transcription.

D. Configure a caller ID policy for the frontline workers.

E. Create a voice routing policy.

ANSWER: A B

Explanation:

Configure an app permission policy that allows the Walkie Talkie app. App permission policies determine which Microsoft, third-party, and custom apps users can access in Teams. The assigned policy must permit the app before the frontline workers can use it.

You should also configure an app setup policy that installs and pins the Walkie Talkie app for the users. App setup policies control which apps are installed and pinned in the Teams client. Pinning the app makes it available from the app bar without requiring each user to locate it manually.

Microsoft documents app availability and client pinning in Manage app permission policies in Microsoft Teams and Manage app setup policies in Microsoft Teams.

QUESTION NO: 65

Your organization plans to deploy 30 Microsoft Teams Rooms devices. Each device must be able to sign in to Teams and join scheduled meetings from its room calendar.

Which two actions should you take? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. Create a resource account for each room.

B. Assign a Microsoft Teams Rooms Pro license to each resource account.

C. Assign a Teams Phone Resource Account license to each resource account.

D. Create a call queue for each room.

E. Assign a Microsoft 365 E3 license to each room resource account.

ANSWER: A B

Explanation:

You should create a resource account for each room and assign a Microsoft Teams Rooms Pro license to each resource account. A Teams Rooms resource account is the account that the room device uses to sign in to Teams. The account has an Exchange Online mailbox that provides the room calendar used for scheduled meetings and one-touch join.

Microsoft Teams Rooms Basic supports up to 25 licensed rooms per tenant. Because this deployment contains 30 rooms, Microsoft Teams Rooms Pro licenses are required for the rooms. Teams Rooms Pro also provides the full Teams Rooms meeting and management capabilities. For more information, see Microsoft Teams Rooms licenses and Create and configure Microsoft Teams Rooms resource accounts.