Lab 01: Manage Microsoft Teams

Student lab answer key

Microsoft 365 user interface

Given the dynamic nature of Microsoft cloud tools, you may experience user interface (UI) changes that were made following the development of this training content. This will manifest itself in UI changes that do not match up with the detailed instructions presented in this lab manual.

The Microsoft World-Wide Learning team will update this training course as soon as any such changes are brought to our attention. However, given the dynamic nature of cloud updates, you may run into UI changes before this training content is updated. **If this occurs, you will have to adapt to the changes and work through them in the lab exercises as needed.**

Lab Scenario

In the labs, of this course, you will assume the role of a Teams Administrator for your corporation. You are asked to ensure the required Teams admin roles are assigned to your pilot team members and check license assignment to users. As part of the Microsoft Teams rollout in your company, you need to make sure the pilot team members are well versed with the usage of Teams admin center, its menus and how to handle day to day administrative tasks. You have implemented Microsoft 365 in a lab environment already and were commissioned to test the creation Microsoft 365 Groups from the M365 admin center and new teams using Teams desktop and web clients. You will also enable access to explore Teams Preview features using Teams update policy. Once the pilot team completes exploring and testing the features in Teams admin center and Microsoft 365 admin center, you need to guide them to follow best practices in creating and configuring naming and expiration policies for the groups and teams while enforcing the restriction on the creation of teams.

You have just started the pilot project.

Objectives

After you complete this lab, you will be able to:

- Assign Teams admin roles to users
- Check license assignment for users
- Understand the Teams admin center and its menus
- Create Microsoft 365 Groups from the M365 admin center
- Create new teams using the Teams desktop client
- Create new teams using the Teams web client
- Configure expiration policies
- Restrict creation of new teams to members of a security group
- Create naming policies
- Enable access to Teams Preview features

Lab Setup

- **Estimated Time:** 100 minutes.

Instructions

Before you start

The labs in this course have been prepared for a Microsoft Teams deployment at your corporation. Your corporation is running a Microsoft 365 cloud-only deployment. The lab environments have been specifically designed in this manner to give you experience managing Microsoft Teams in a Microsoft 365 deployment.

1. Review installed applications

Once you signed in to the environment, observe the start menu, and verify following applications have been installed:

- Microsoft Teams

2. Review Microsoft 365 tenant

You will also be provided with a Microsoft 365 tenant with the following highlights:

- The username of the Global Administrator youruser**@<YourTenant>.onmicrosoft.com**.
- **<YourTenant>.onmicrosoft.com** - This is the domain associated with the Microsoft 365 tenant that was provided by the lab hosting provider. The first part of this domain name (<YourTenant>) is the unique tenant ID provided by the lab hosting provider. The <YourTenant> portion of the tenant ID, which is the tenant suffix ID, will be unique for each student.
- Throughout the lab exercises for this course, if you navigate to the Microsoft 365 admin center, make sure the slider in the upper right corner is set to **The new admin center**. If you can read **Try the new admin center**, select the slider, and activate it.

  IMPORTANT: The instructions that are provided in the lab exercise for this course are based on the new Microsoft 365 admin center UI and not the classic UI.

Exercise 1: Prepare Teams admin roles and licenses

In the first exercise, you will assign required administrative roles to users and check license assignments for the Teams license. To perform these tasks, you will use default tenant global admin.

Task 1 - Assign Teams admin roles to users

In this task, you will use the default global admin to sign in to the Microsoft 365 admin center and assign several Teams admin roles to different users. This task is crucial for later tasks and exercises as you will perform most of the tasks in the context of your user account.

1. Browse to Microsoft 365 admin center (https://admin.microsoft.com/).

- Browse to the **Microsoft 365 admin center** at **https://admin.microsoft.com/** with the Global admin credential (youruser**@<YourTenant>.onmicrosoft.com**.).

2. To assign **Teams admin** role

   - Select the navigation menu in the upper-left and select **Users** and **Active users** from below it.

   - In the Active user's list, search and select **a user that does not have the Teams Admin role**, to open the right-side settings pane.

   - In the settings below the Account tab, select **Manage roles**.

   - On the **Manage admin roles** pane, select **Admin center access** and scroll down to expand **Show all by category** to reveal all available roles.

   - Select **Teams Administrator** checkbox then select **Save changes**. You will see the message **Admin roles updated** on the upper part of the pane to confirm the update. Close the **Manage admin roles** pane by selecting the X button on the top right side of the pane.

3. To assign **Teams device admin** role to **Patti Fernandez**

   - Repeat the same steps as above, in the **Active users list**, search and select **Patti Fernandez** and assign **Teams Device Administrator** role to **Patti Fernandez**.

4. To assign **Teams communication Support engineer** role to **Allan Deyoung**

   - Repeat the same steps as above and assign **Teams communication support engineer** role to **Allan Deyoung**.

Proceed to the next task.

Task 2 – Check license assignment of your users

In this task, you will check the license assignment of all users participating in the pilot. At the end of the task, you will confirm that all pilot users are licensed correctly and Alex Wilber's location is updated to Canada as preparation for a later task.

1. browse to Microsoft 365 admin center (https://admin.microsoft.com/).

2. Update **Alex Wilber's** location to **Canada.**
    - On the **Users** > **Active users** page, select the name of **Alex Wilber**.
    - Select **Licenses and Apps** tab.
    - Select the dropdown menu under **Select location**, and update to **Canada**.
    - Select **Save changes**.
3. Check **Alex Wilber's** licenses
    - On the same tab, under **Licenses** section, verify that **Enterprise Mobility + Security E5** and **Office 365 E5** are both selected.
    - Select **Apps** to expand All licenses.
    - Scroll down the list of all apps, and verify **Microsoft Teams** is selected.
4. You can repeat the same steps to check other users' licenses. Do not change their locations.

You have successfully validated that all Users participating in the pilot own Teams licenses and are ready to start working with Teams. You have also changed the location of Alex Wilber to Canada, as a preparation for a later task. Continue with the next task.

You have finished the first exercise, and you can continue with the next one.

Exercise 2: Explore Teams management tools

In this exercise, you will explore the Teams admin center, required to manage teams, policy packages, calling features, and all other settings for Teams in your tenant. You can perform most of the tasks possible from the Teams admin center. You can create scripts for automation and even access several settings not available in the GUI.

To perform these tasks, you will use your account (youruser@<*YourTenant*>.onmicrosoft.com).

Task 1 - Explore Teams admin center

You will review the available settings for managing Teams in the Teams admin center.

1. Browse to Teams admin center (https://admin.teams.microsoft.com)

(your@<YourTenant>.onmicrosoft.com).

Note: You can use **InPrivate window** of Microsoft Edge for logging in with different credentials.

2. In left navigation of the Teams admin center, select **Teams** > **Manage teams**. You will see the teams in your organization once created.
3. In left navigation of the Teams admin center, select **Teams** > **Teams policies**. You can see the default Teams policy named **Global (Org-wide default)**.

You can explore other settings to familiarize various controls in the Teams admin center.

You have successfully explored several available menus from the Teams admin center for managing teams and configuring policies in your tenant.

Exercise 3: Create groups and teams

In this exercise, you will create a Microsoft 365 group from the Microsoft 365 admin center and create a team from the Teams desktop client and the web client.

Task 1 - Create a Microsoft 365 Group

You will create a new Microsoft 365 Group named "IT-Department," and then add the pilot members serving as a basis for your future teams and licensing.

1. Browse to the **Microsoft 365 admin center** (https://admin.microsoft.com/) (youruser@<YourTenant>.onmicrosoft.com).
2. In the Microsoft 365 admin center, select **Teams & groups** > **Active teams & groups**.
3. On the **Active teams and groups** page, select **Add a group**.
4. Follow the **Add a group** wizard with the following information:
    - Group type: Select **Microsoft 365 (recommended)**
        - Select **Next**
    - Basics:

        - Name: **IT-Department**
        - Description: **All staff of the IT-Department**
        - Select **Next**
    - Owners:
        - Select **+ Assign owners**
        - Search and select **Joni Sherman**
        - Select **Add(1)**, and then select **Next**.
    - Members:
        - Select **+ Add Members**, and add the following users:
            - Patti Fernandez
            - Allan Deyoung
        - Select **Add(3)**, and then select **Next**.
    - Settings:
        - Enter **IT-Department** for Group email address.
        - Privacy: **Private**
        - Uncheck **Create a team for this group**.
        - Select **Next**
5. Select **Create group** > **Close**.
6. Wait a moment and select **Refresh** until the group is visible. You will see there is no Teams icon in the **Teams status** column.
7. Select the **IT-Department** group to review the settings and members.

The new Microsoft 365 Group with the name "IT-Department" was successfully created. Close the browser window and continue to the next task.

Task 2 - Create a new team by using the desktop client

To test the self-service capabilities of Teams, in this task, **Alex Wilber** will sign in to the Teams Desktop client, create a new team with the name **Teams Rollout** and add all members participating in the Teams evaluation project.

1. Connect with the credentials that have been provided to you.

2. Select the **Teams** icon on the taskbar to start the Teams, desktop client.

3. Select on **"Get Started"** and Sign in as **Alex Wilber** (AlexW@<YourTenant>.onmicrosoft.com). At the 'Stay signed in to all your apps' window, select **No, sign in to this app only**.

   Note: If you don't have Alex's password, you can reset Alex's password with the following steps:

   i. Login to **Microsoft 365 Admin Center** as **MOD Administrator**.
   ii. On the **Users > Active users** page, select the name of **Alex Wilber**.
   iii. Select **Reset password** from the top, then select **Automatically create a password** and uncheck **Require this user to change their password when they first sign in** and **Reset password**.
   iv. Use the password under column Password to login.

   Note: You might need to download and install the latest Teams, desktop client. If so, select **Update Teams** and follow the installation guideline - Select **Download for desktop** > **Download Teams Run**.

4. In the Teams desktop client, select **Teams** from the left menu.

5. Select **Join or create a team** from the lower-left corner.

6. Select **Create team** > **From scratch** > **Public**. Enter the team name **Teams Rollout** and select **Create**.

7. On the **Add members to Teams Rollout** window, enter the following names and select **Add**.

   - Joni Sherman
   - Lynne Robbins
   - Diego Siciliani

8. Select the dropdown menu next to Joni Sherman and switch from **Member** to **Owner**.

9. Select **Close**.

You have successfully created a new team from the Teams desktop client added the project team members, and you have made Joni Sherman a team owner.

Task 3 - Create a new team by using the web client

In this task, **Lynne Robbins** will continue testing the self-service capabilities of Teams by using the Teams web client to create another team with the name **Sales**. She will also add **Alex Wilber** as a member.

1. Browse to the **Microsoft Teams web client** at **https://teams.microsoft.com** and sign in (youruser@<YourTenant>.onmicrosoft.com).

2. Select **Use the Web app instead** if prompted to download the Teams Desktop app. At the 'Stay signed in to all your apps' window, select **No, sign in to this app only**.

3. Select **Join or create a team** from the lower-left corner.

4. Select **Create team** >**From scratch** > **Private**. Enter the team name **Sales** and select **Create**.

5. On the **Add members to Sales** window, enter the following names and select **Add** > **Close**.

    - Alex Wilber

The newly created team is displayed in the list of your teams. You have successfully created a new team with the Teams web client.

Exercise 4: Implement lifecycle management and governance for Microsoft Teams

Your organization has started the planning process for Microsoft 365 services adoption. You are assigned a Teams admin role to plan Teams governance. Since Teams relies on Microsoft 365 groups, you need to plan governance procedures for Microsoft 365 groups, including creating **Microsoft 365 groups expiration policies**,

configuring **Microsoft 365 Group creation policy permissions**, configuring and testing **Microsoft 365 Groups naming policies**.

Task 1 - Create and assign an expiration policy

Based on the organization's requirement, unneeded groups should be deleted automatically after 90 days. To evaluate the expiration feature for Teams, you will configure a group expiration policy that will expire the **Teams Rollout** group after 90 days.

1. Browse to Azure AD admin center (https://aad.portal.azure.com/)
2. On the left navigation pane, select **Azure Active Directory** > **Groups**.
3. On the **Groups** page, select **Expiration**.
4. On the **Groups | Expiration** page, configure the following settings:
    - In the dropdown menu of **Group lifetime (in days)**, select **Custom** and enter **90** to the text box.
    - In the text box right from **Email contact for groups with no owners**, enter (youruser@<YourTenant>.onmicrosoft.com).
    - Right from **Enable expiration for the Office 365 groups**, select **Selected**.
    - Select **+ Add** to open the **Select groups** right-side pane.
    - In the **Select groups** pane, type **Teams Rollout** into the textbox and select the group.
    - Use the **Select** button on the lower end of the right-side pane to apply the policy to the **Selected group**.
    - Back on the **Groups | Expiration** page, select **Save**.

You have successfully created a new expiration policy and configured the **Teams Rollout** team to expire after 90 days. If the team doesn't have an owner after 90 days, Joni Sherman will be notified about the expiration.

Task 2 - Configure a group creation policy

You are an administrator for your Team's organization. You need to limit which users can create Microsoft 365 groups. You will create a security group named **GroupCreators** which only the members of the group can create Microsoft 365 groups.

1. Browse to the **Microsoft 365 admin center** (https://admin.microsoft.com/) as the Global admin (youruser@<YourTenant>.onmicrosoft.com).

2. In the Microsoft 365 admin center, select **Teams & groups** > **Active teams & groups**.

3. On the **Active teams and groups** page, select **Add a group**.

4. Create a security group.

   Follow the **Add a group** wizard with the following information:

   - Group type: Select **Security** > **Next**
   - Basics:
     - Name: **GroupCreators**
     - Description: **Users who can create Microsoft 365 Groups for new teams**
     - Select **Next**
   - Finish: Select **Create Group** and then select **Close**
   - Back to **Active teams & group** page, select **Security** tab and Select on the security group **GroupCreators** you just created.
   - Select **Members** tab to configure the **Owners** and **Members**.
     - Owners: Select **View all and manage owners** and select **+ Add owners.**
     - Members: Select **View all and manage members** > **+ Add members**, and add the following users:
       - Joni Sherman
       - Alex Wilber

5. Restrict the Microsoft 365 groups creation to the security group.

6. Test the newly configured settings.

i. Test the credentials that have been provided to you.

ii. Test as **Alex Willber** from Teams desktop client, notice when select **Join or create a team**, there are options for **Create team** and **Join a team with a code**.

iii. Test as **Lynne Robbins** from Teams web client, notice when select **Join or create a team**, only one option **Join a team with a code** is available.

> **Note:** When you are still able to create a new team, wait several minutes for the new configuration to take effect on your users.

In this task, you have successfully created a new security group and configured Azure AD settings to restrict the creation of new groups to members of this group only. At the end of the task, you have successfully tested the new group creation restrictions.

Task 3 - Configure a new naming policy

As part of your Teams planning project, you will configure the naming policy where each new Microsoft 365 group or team needs to comply with the organization's regulations on naming objects. Each group name should start with the letters **Group** and end with the **Country** attribute of the owners' location. Furthermore, there is an internal regulation that forbids using the following specific keywords in Teams names: **CEO**, **Payroll**, and **HR**.

1. Browse to Azure AD admin center (https://aad.portal.azure.com/) as **MOD Administrator**.

2. On the left navigation pane, select **Azure Active Directory** > **Groups**.

3. On the **Groups** page, select **Naming policy**.

4. Configure **Blocked words**

    i. Under the **Blocked words** tab on the **Groups | Naming policy** page, select **Download** to download a sample file.

    ii. Navigate and right-select the downloaded file **BlockedWords.csv** and select **Open with** > **Notepad**.

    iii. Type **CEO,Payroll,HR** replacing the empty quotes in the Notepad window, and saving the file.

iv. Back to the **Groups | Naming policy** page, upload the saved .csv file under **3. Upload your .csv file** by selecting **Select a file** box or the folder icon.

v. Select **Save** to apply the new blocked words setting.

5. Configure **Group naming policy**

i. On the **Groups | Naming policy** page, select the **Group naming policy** tab.

ii. Add **Group_** string as prefix

a. Select the checkbox **Add prefix**.
b. Select the dropdown menu of **Select the type of prefix** and choose **String**.
c. Enter **Group_** to the text box.

iii. Add **Country or region** string as the suffix

a. Select the checkbox **Add suffix**.
b. Select the dropdown menu of **Select the type of suffix**, choose **String**, and enter _ to the text box.
c. Select the dropdown menu of **Select the type of suffix**, choose **Attribute**, and Select **Country or region** from the dropdown menu.

iv. Select **Save** to apply the new blocked words setting.

In this task, you have configured a naming policy that will block specific words to be used in a Microsoft 365 group name, as well as you have configured a new naming policy for the names of Microsoft 365 groups and teams.

Task 4 - Test the new naming policy

You need to test the newly created naming policy to see its effects in your pilot environment. In the following task, you will try to create a new team and see the configured naming policy template completing the configured name for your new team.

Note: It can take up to 24 hours till the blocked words setting will take effect. Therefore, you will only test the configured naming policy, which takes effect immediately.

1. Open the **Teams desktop client** (https://teams.microsoft.com/) (youruser@<YourTenant>.onmicrosoft.com)
2. In the Teams desktop client, select **Teams** from the left menu.
3. Select **Join or create a team** from the lower-left corner.
4. Select **Create team** > **From scratch** > **Public**.
5. Enter **Afterwork** for the **Team name**.

   Below the entered name, you can see the configured prefix and suffix for new teams.
6. Select **Create** to create the new team.
7. Add **Lynne Robbins** to the team member.
8. Review the name of the newly created team.

You have successfully tested the naming policy for managing the prefix and suffixes of user-created teams.

Task 5 - Delete the naming policy

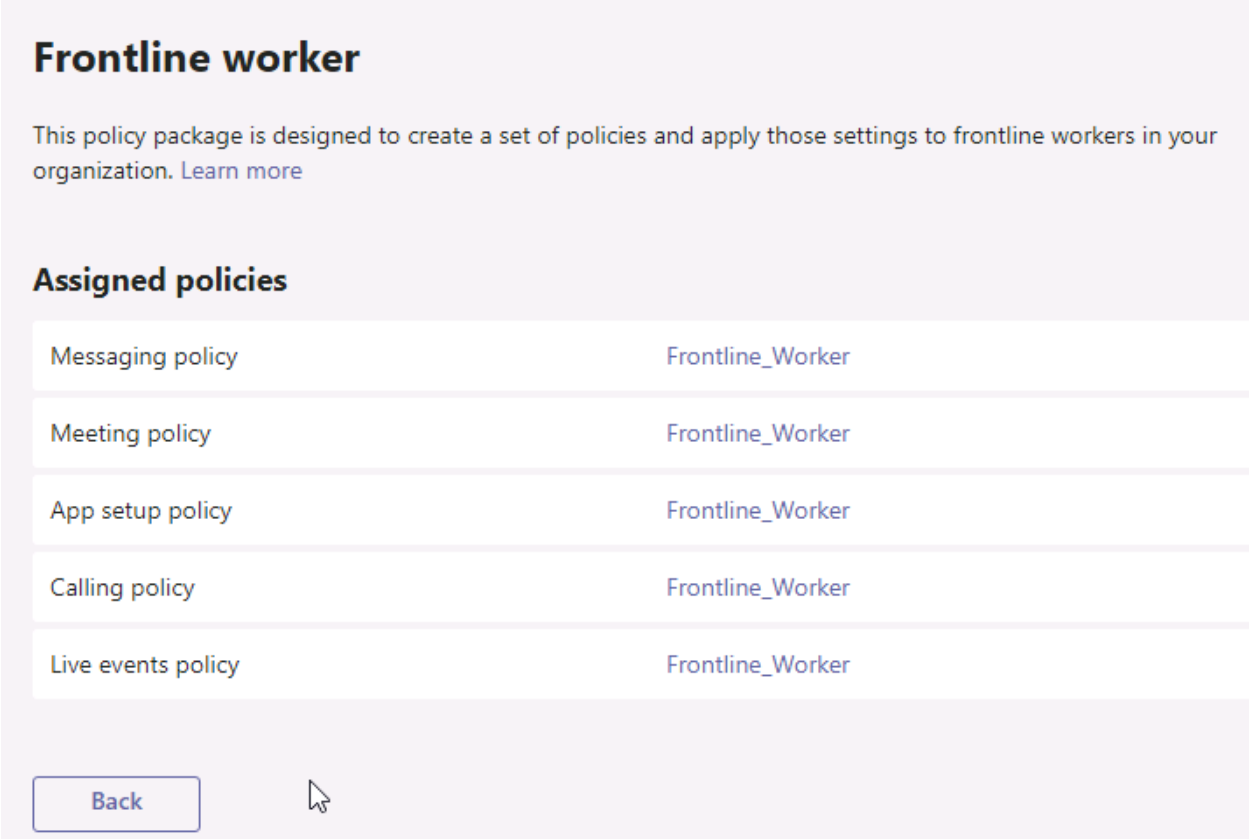
You can remove the naming policy after the test. In the following task, you will remove the naming policy you just created.

1. Browse to Azure AD admin center (https://aad.portal.azure.com/)
2. On the left navigation pane, select **Azure Active Directory** > **Groups**.
3. On the **Groups** page, select **Naming policy**.
4. On the **Groups | Naming policy** page, select **Delete policy** > **Yes**.

Task 6 – Manage policy packages

To avoid administrative overhead with managing large numbers of policies individually for groups of different users, you need to evaluate using policy packages to group policies into logical units. In this task, you need to review the default policy packages and change a default policy package for first-line workers.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) as **your user** (youruser@<YourTenant>.onmicrosoft.com).
2. In the left navigation of the Teams admin center, select **Policy packages**.
3. On the **Policy packages** page, select **Frontline worker (default)** policy package.



4. Update Messaging policy in **Frontline worker** policy package.
    i. Select **Frontline_Worker** right from **Messaging policy**.
    ii. Select **Edit** from the upper right corner.
    iii. Turn **On** the setting - **Send urgent messages using priority notifications** and select **Save**.
5. Update Calling policy in **Frontline worker** policy package.
    i. Back to **Policy packages** page.
    ii. Select **Frontline worker (default)** from the list again.
    iii. Select **Frontline_worker** right from **Calling policy**.

iv. Turn **On** the setting - **Prevent toll bypass and send calls through the PSTN**.

v. Update **Busy on busy when in a call** to **Enabled**.

vi. Select **Save**.

6. Navigate to **Policy Packages** from the left navigation pane.

7. Make sure **Frontline worker** policy package is checked.

8. Select **Manage users** from the top menu.

9. Type **Allan** into the search box, select **Add** right from **Allan Deyoung** and **Apply**.

10. Check the policy assignment.

    i. Select **Users** > **Manage users** from the left-side pane.

    ii. Select **Allan Deyoung** and select **Policies** tab.

    iii. You can see the **Frontline worker** under policy package section.

You have successfully modified included policies from an existing policy package and assigned the package to a single user. This will help you assign the same set of policies to a group of users working in the same role or requiring the same access.

Exercise 5: Enable access to Teams public preview features using Teams update policies

In this exercise, you will configure users to explore and evaluate upcoming features using Teams update policies. Public preview is enabled on a per-user basis, and Update policies are used to manage Teams and Office preview users who will see pre-release or preview features in the Teams app.

Task 1 - Create a custom Update policy

1. Browse to **Teams Admin Center** https://admin.teams.microsoft.com

   Note: You can use **InPrivate window** of Microsoft Edge for logging in with different credentials.

2. In left navigation of the Teams admin center, select **Teams** > **Teams update policies**.

3. Select **+ Add**
4. Enter the following information:
    - Name: **Enable Preview features**
    - Description: **Enable Teams public preview**
    - Show preview features: select **Enabled**
    - Select **Apply**

You now completed creating a custom **Teams Update policy.**

Task 2 - Assign the custom Update policy to users

Now you need to assign the custom Update policy to specific users because it doesn't over-write the global policy.

1. Go to **Teams admin center** > **Teams** > **Teams update policies**.
2. Select the custom Update policy **Enable Preview features**.
3. Select **Assign users**.
4. Search and select **Add** next to the following pilot users:
    - Alex Wilber
    - Lynne Robbins
    - Diego Siciliani
5. Select **Apply** to assign the custom update policy created in task 1.

END OF LAB

Lab 02: Prepare the environment for a Microsoft Teams deployment

Student lab answer key

Lab Scenario

In the labs of this course, you will assume the role of the Global Administrator for your company. Your organization is planning to deploy Microsoft Teams. Before starting the deployment, the IT department is gathering business requirements about data security and compliance, including how the data shared in Teams be regulated according to the organization's compliance requirements. Also there are concerns about the current network infrastructure to meet the requirements for Microsoft Teams services. Therefore, you need to analyze the current network infrastructure and perform bandwidth calculations. Based on your estimation, you can provide recommendations to the networking team.

After you complete the planning process, you will protect Teams from threats, and configure Teams to meet your organization's compliance requirements.

Objectives

After you complete this lab, you will be able to:

- Configure guest access in Azure and Teams
- Review Access to a resource
- Activate, create and assign sensitivity labels
- Activating Safe Attachments for SharePoint, OneDrive, and Teams
- Create, configure and test retention policies
- Create and test a DLP policy to protect GDPR content
- Calculate the network bandwidth capacity for a Teams deployment

- Work with the Microsoft 365 network connectivity test tool on a client

Lab Setup

- **Estimated Time:** 120 minutes.

Instructions

Exercise 1: Manage guest access for Microsoft Teams

In this exercise, you will test the guest access features in Microsoft 365. To do so, you will configure guest access in Azure AD, add a new external guest user and revoke the guest access by using access reviews.

Task 1 - Review guest access settings (optional)

1. Browse to Azure AD admin center (https://aad.portal.azure.com/)
2. In left navigation of the Azure AD admin center, select **Users**> **User settings** > **Manage external collaboration settings** under the External users. Review the following settings for external users at the Azure AD level:
    - **Guest user access**: Guest users have limited access to properties and memberships of directory objects.
    - **Guest invite settings**: Anyone in the organization can invite guest users including guests and non-admins (most inclusive).
    - **Collaboration restrictions**: Allow invitations to be sent to any domain (most inclusive)
3. Browse to Microsoft 365 admin center (https://admin.microsoft.com/).
4. In the left navigation of the Microsoft 365 admin center, select the **Show all** and select **Settings** > **Org settings**.
    - Under the **Services** tab, select **Microsoft 365 Groups**. Make sure the checkbox is selected for **Let group owner add people outside your organization to Microsoft 365 Groups**. Close the **Microsoft 365 Groups** page by selecting **X** button.

- Under the **Security & privacy** tab, select **Sharing**. Make sure the checkbox is selected for **Let users add new guests to the organization**.

You have now reviewed guest access settings across different admin centers. You are ready to invite the guest for collaboration.

Task 2 - Configure guest access in Teams

Now that you have explored the Teams admin center it is time to configure the first setting. Since this task will take some time to replicate through the tenant, you will configure the guest user access for Microsoft Teams right now, so it is available for later use.

1. Browse to Teams admin center (https://admin.teams.microsoft.com)
2. In the left navigation of the Teams admin center, select **Users** > **Guest access**.
3. On the **Guest access** page, check if **Allow guest access in Teams** is enabled. If not, select **On**.
4. Scroll down and under **Messaging** section, disable **Delete sent messages**
5. Scroll down and select **Save**.

You have now successfully activated guest access and disallowed guests to delete their sent messages for Teams in your tenant.

Task 3 - Add a guest to a team

In this task, you will add a guest user by inviting the guest to the team **Group_Afterwork_United States** you created from Lab 1.

You will change the default settings for inviting/creating guest users and then add your personal Outlook.com account as a guest user to your tenant.

Note: You will need an Outlook.com account for this exercise. If you don't have an outlook account, you can create a new account from **https://outlook.com**.

1. Open the **Teams desktop client** (https://teams.microsoft.com/)

   (youruser@<YourTenant>.onmicrosoft.com)

2. Add the guest to **Group_Afterwork_United States** team.

- Select **Teams** > Select **...** next to the **Group_Afterwork_United States** team.
- Select **Add member** and enter your outlook account.
- You will see a message **add <Your outlook account> as a guest**. Select the message and select **Add**.

3. Accept the guest invite
    - Open a **New InPrivate window** and check the email with subject **You have been added as a guest to Your organization in Microsoft Teams** from **Outlook Web Portal** (https://outlook.live.com/owa/).
    - Select **Open Microsoft Teams** from the email. You will be redirected to the sign-in page with a permission consent request.
    - Select **Accept** and sign in to Teams web client with your outlook account.
    - From the Teams client, select **Teams**, you will see the team **Group_Afterwork_United States**.
4. Test the guest access
    - Under the team **Group_Afterwork_United States**, select **General** channel, select **New conversation** and send the message: **Hello!**.
    - Select **...** of the message you just posted. Notice there's no **Delete** option.

You have successfully invited a guest to a team and validated the guest access setting from the previous task.

Task 4 - Create access reviews

As a part of your system administrator role, you need to review access to resources in your tenant regularly. You can do that by creating an access review.

1. Browse to Azure AD admin center (https://aad.portal.azure.com/).
2. Create an access review to monitor guest users.

    In left navigation of the Azure AD admin center, select **All Services** and on right pane select **Identity Governance** > select the **Access Review** in the middle pane

and select **+ New access review**. Follow the wizard with the following information:

i. On the **Review type** tab:

- In the **Select what to review** section, select **Teams + Groups**.
- In the **Select review scope** section, select **All Microsoft 365 groups with guest users.**
- In the **Scope** section, select **Guest users only**.
- Select **Next: Reviews**.

ii. On the **Reviews** tab:

- In the **Select reviewers** section, select **Group owner(s)**.* In the **Specify recurrence of review** section, select **Weekly** and keep rest as default.
- Select on **Next: Settings**.

iii. On the **Settings** tab, leave the settings as default. Select on **Next: Review+Create** > **Create**.

3. Review the access review dashboard from Azure AD.

i. On the **Identity Governance | Access reviews** page, you will see an access review report named **Review guest access across Microsoft 365 groups**

ii. Wait for a few minutes, when the **Status** of the report shows as **Active**, select the name of the report - **Review guest access across Microsoft 365 groups**.

iii. On the **Review guest access across Microsoft 365 groups | Overview** page, select **Group_Afterwork_United States** under the group name.

iv. On the **Group_Afterwork_United States | Overview** page, you can see there is one user shown under **Not reviewed** category.

4. Review the access review and approve the guest user.

i. Browse to the **Outlook.com** (https://outlook.office.com/) (youruser@<YourTenant>.onmicrosoft.com). You can open an InPrivate window.

ii. Check the email with the subject **Action required: Review group access**.

iii. Select **Start review >** in the content of the email.

iv. From the **My Access** (Https://myaccess.microsoft.com) page, select **Review guest access across Microsoft 365 groups**.

v. On the **Review guest access across Microsoft 365 groups** page, select the guest account and select **Approve**.

vi. From the **Approve continued access** window, enter **Approved.** to the textbox, and select **Submit**

You have successfully created an access review and approved a guest user in your tenant.

Exercise 2: Implement security for Microsoft Teams

In this exercise, you will increase the security level in your organization by configuring Safe Attachments to ensure that no malicious content is sent through documents shared in Teams by blocking attachments that contain malware.

Task 1 - Configure Safe Attachments for Microsoft Teams

Users in your organization are using Microsoft Teams for communication and collaboration. Business managers are concerned that documents that are shared within Microsoft Teams may contain malware. You will need to ensure that no malicious content is sent through documents shared in Teams by configuring Safe Attachments that block documents that contain malware.

1. Browse to Microsoft 365 Defender portal (https://security.microsoft.com/).

2. In left navigation of the Microsoft 365 Defender portal, expand **Email & Collaboration** section, select **Policies & rules** > **Threat policies** > **Safe Attachments** in the **Policies** section.

3. On the Safe attachments page, select **Global settings**.

4. In the Global settings flyout that appears, **Turn On** the toggle under **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams**.

5. Select **Save**.

In this task, you have activated Safe Attachments scanning for SharePoint, OneDrive, and Microsoft Teams that block documents that contain malware.

Exercise 3: Implement compliance for Microsoft Teams

Before deploying Microsoft Teams in your organization, you need to evaluate Microsoft Team's compliance features to meet the organization's requirements.

Task 1 – Activate and Configure sensitivity labels for Teams

After activating sensitivity labels for groups, you will now create three sensitivity labels. In this task, you will create and update three sensitivity labels **General**, **Internal**, and **Confidential**. For each of them, you will create appropriate user and admin descriptions.

1. Browse to Microsoft Purview Portal https://compliance.microsoft.com/).

2. In the left navigation of the Microsoft Purview compliance portal, select **Information protection** and select the **Labels** tab.

3. Select **Turn on now** next to the following warning message to activate content processing in Office online files.

   Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn it on here, but note that additional configuration is required for Multi-Geo environments. Learn more

4. Update the first sensitivity label - **General**.

   Select the **General** label and select the **Edit label** button, follow the wizard with the following information and select **Next** after each step:

   i. In the **Name & description** section, enter the following information:

      - **Name**: Leave unchanged
      - **Display name**: General

- **Description for users**: Leave unchanged
- **Description for admins**: General information without encryption, marking or sharing restriction settings activated.

ii. In the **Scope** section, select **Items** and **Groups & sites**.

iii. In the **Items** and **Auto-labeling** sections, leave the settings as default.

iv. In the **Groups & sites** section, select both checkboxes.

- **Privacy and external user access settings**
- **External sharing and Conditional Access settings**

v. In the **Privacy & external user access** section,

- Select **None** under Privacy section.
- Check the checkbox of **Let Microsoft 365 Group owners add people outside your organization to the group as guests** under External user access section.

vi. In the **External sharing & conditional access** section,

- Select **Control external sharing from labeled SharePoint sites** and select **Anyone**.
- Select **Use Azure AD Conditional Access to protect labeled SharePoint sites** and select **Allow full access from desktop apps, mobile apps, and the web**.

vii. In the **Schematized data assets (preview)** section, leave the settings as default and select **Next**.

viii. Select **Save label** > **Done**.

ix. On the **Choose sensitivity labels to publish** page, select **Cancel**.

5. Create the second sensitivity label - **Internal**.

   Select **+ Create a label**, follow the wizard with the following information and select **Next** after each step:

   i. In the **Name & description** section, enter the following information:

   - **Name**: Internal

- **Display name**: Internal
- **Description for users**: Internal information with sharing protection
- **Description for admins**: Internal information with moderate encryption, marking and sharing restriction settings activated

ii. In the **Scope** section, select **Items** and **Groups & Sites**

iii. In the **Items** section, select both checkboxes.

- **Encrypt items**
- **Mark items**

iv. In the **Encryption** section,

- Select **Configure encryption settings**
- Assign permissions now or let users decide: **Assign permissions now**.
- User access to content expires: **Never**.
- Allow offline access: **Always**.
- Select **Assign permissions**, and select **+ Add all users and groups in your organization**.
- Scroll down and select **Save** to apply the changes.

v. In the **Content marking** sections,

- Select the slider and the checkbox **Add a watermark**.
- Select **Customize text** and enter the following to the **Watermark text** box: **Internal use only**
- Click **Save** to apply the changes.

vi. In the **Auto-labeling** section, leave the settings as default.

vii. In the **Groups & sites** section, select both checkboxes.

- **Privacy and external user access settings**
- **External sharing and Conditional Access settings**

viii. In the **Privacy & external user access** section, select **None**.

ix. In the **External sharing & device access** section

- Select **Control external sharing from labeled SharePoint sites** and select **Existing guests**.
- Select **Use Azure AD Conditional Access to protect labeled SharePoint sites** and select **Allow limited, web-only access**.

x. In the **Schematized data assets (preview)** section, leave the settings as default.

xi. Select **Create label** > **Done**.

xii. On the **Choose sensitivity labels to publish** page, select **Cancel**.

6. Update the second sensitivity label - **Confidential**

   Select the **Confidential** label and select the **Edit label** button, follow the wizard with the following information and select **Next** after each step:

   i. In the **Name & description** section, enter the following information:

   - **Name**: Leave unchanged
   - **Display name**: Confidential
   - **Description for users**: Leave unchanged
   - **Description for admins**: Confidential information with all restrictive encryption, marking and sharing settings activated

   ii. In the **Scope** section, select **Items** and **Groups & Sites**

   iii. In the **Items** section, select both checkboxes.

   - **Encrypt items**
   - **Mark items**

   iv. In the **Encryption** section,

   - Select **Configure encryption settings**
   - Assign permissions now or let users decide: **Assign permissions now**.
   - User access to content expires: **Never**.
   - Allow offline access: **Never**.
   - Select **Assign permissions**, and select **+ Add all users and groups in your organization**.

- Scroll down and select **Save** to apply the changes.

v. In the **Content marking** sections,

- Select the slider and the checkbox **Add a watermark**.
- Select **Customize text** and enter the following to the **Watermark text** box: **Confidential.**
- Click **Save** to apply the changes.

vi. In the **Auto-labeling** sections, leave the settings as default.

vii. In the **Groups & sites** section, select both checkboxes.

- **Privacy and external user access settings**
- **External sharing and Conditional Access settings**

viii. In the **Privacy & external user access** section, select **Private**.

ix. In the **External sharing & conditional access** section

- Select **Control external sharing from labeled SharePoint sites** and select **Only people in your organization**.
- Select **Use Azure AD Conditional Access to protect labeled SharePoint sites** and select **Block access**.

x. In the **Schematized data assets (preview)** section, leave the settings as default.

xi. Click **Save label** > **Done**.

xii. On the **Choose sensitivity labels to publish** page, select **Cancel**.

7. Publish sensitivity labels, after performing each step select **Next** (if required).

i. On the **Information protection** page, select **label policies** tab.

ii. Select the **Global sensitivity label policy** and select the **Edit policy** button.

iii. In the **Choose sensitivity labels to publish** window, select the **Edit** Link.

iv. In the **Sensitivity labels to publish** window, check all labels and select **Add**.

v. In the **Publish to users and groups** section, keep the default settings.

vi. In the **Policy Settings** section, keep the default settings.

vii. In the **Apply this a default label to documents** section, select **General** in the dropdown menu under **Apply this label by default to documents**.

viii. In the **Apply a default label to emails** section, select **General** in the dropdown menu under **Apply this label by default to emails**.

ix. In the **Policy settings for Sites and Groups** section, select **General** in the dropdown menu under **Apply this label by default to groups and sites**.

x. In the **Apply a default label to Power BI content (preview)** section, select **General** in the dropdown menu under **Apply this label by default to Power BI content**.

xi. In the **Name** section, leave unchanged

xii. Select **Submit** > **Done**.

In this task, you have created and published three new sensitivity labels available for all users, which can be assigned to new and existing teams.

Task 2 - Assign sensitivity labels to teams

Once the sensitivity labels are created and published, users can now assign them to teams. Furthermore, users can modify assigned labels if needed. In this task, you will assign the **Internal** label to the **Teams Rollout** team.

Note: It can take several minutes till the newly created sensitivity labels are available to users.

1. Open Teams.
2. On the Teams overview select the **...** on the right side next to the Team "**Teams Rollout,"** then select **Edit team** from the dropdown list.
3. On the **Edit "Teams Rollout" team** window, select the dropdown menu below Sensitivity and select **Internal**.
4. Select **Done** to save the changes.

You have successfully applied a sensitivity label to an existing team. The configured settings of the Internal label are now applied to the Teams Rollout team. Continue with the next task.

Task 3 – Test external access with sensitivity labels (optional)

In this task, you will try to add a guest user to an internal team.

1. Open the Microsoft Teams.
2. On the Teams overview select **...** right next to the Team "**Teams Rollout"** then select **Add member** from the dropdown list.
3. On the **Add members to Teams Rollout** page, enter the name of the guest user you just invited.
4. You will not be able to find the guest user, because guest users are restricted from this team.
5. Select **Close.**

You have successfully tested the sensitivity labels setting to prevent guest access to a protected team and you can confirm, the labels are working as predicted.

Task 4 - Create a new retention policy to retain content

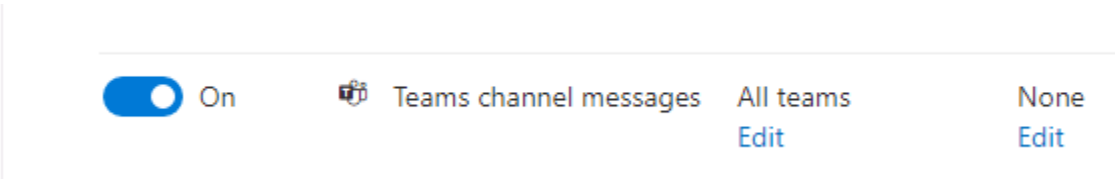
Teams retention settings are very important for managing the lifecycle of company data, therefore, the capabilities of retention policies need to be evaluated in the Teams pilot. In this task, you will create a new retention policy that retains the Teams channel messages of the **Sales** team for **7 years** after the last modification.

1. Browse to Microsoft Purview Portal(https://compliance.microsoft.com/).
2. In the left navigation of the Microsoft Purview Portal, select **Data lifecycle management**.
3. On the **Data lifecycle management** page, under **Retention policies** tab, select **+ New retention policy** to create a new retention policy.
4. Follow the **Create retention policy** wizard with the following information:
    i. In the **Name** section, enter the following information

- **Name**: Sales retention policy
- **Description**: Retention policy for Sales department that will retain channel messages for 7 years.
- select **Next**

ii. In the **Type** section, select **Static** and select **Next** then configure the following settings:

- **Exchange email**: Off
- **SharePoint sites**: Off
- **OneDrive accounts**: Off
- **Microsoft 365 Groups**: Off
- **Skype for Business**: Off
- **Exchange public folders**: Off
- **Teams channel messages**: On
- **Teams chats**: Off
- **Teams private channel messages**: Off
- **Yammer community message**: Off
- **Yammer user messages**: Off
- Select **Edit** in the **Included** column (under the current *All teams* choice) for the **Teams channel messages** line to open the right-side pane.
- Select the checkbox left from **Sales** and select **Done**.



iii. In the **Retention settings** section, select **Next**.

5. In the **Finish** section, review your settings and select **Submit**.

6. Select **Done**. Leave the browser open for the next task.

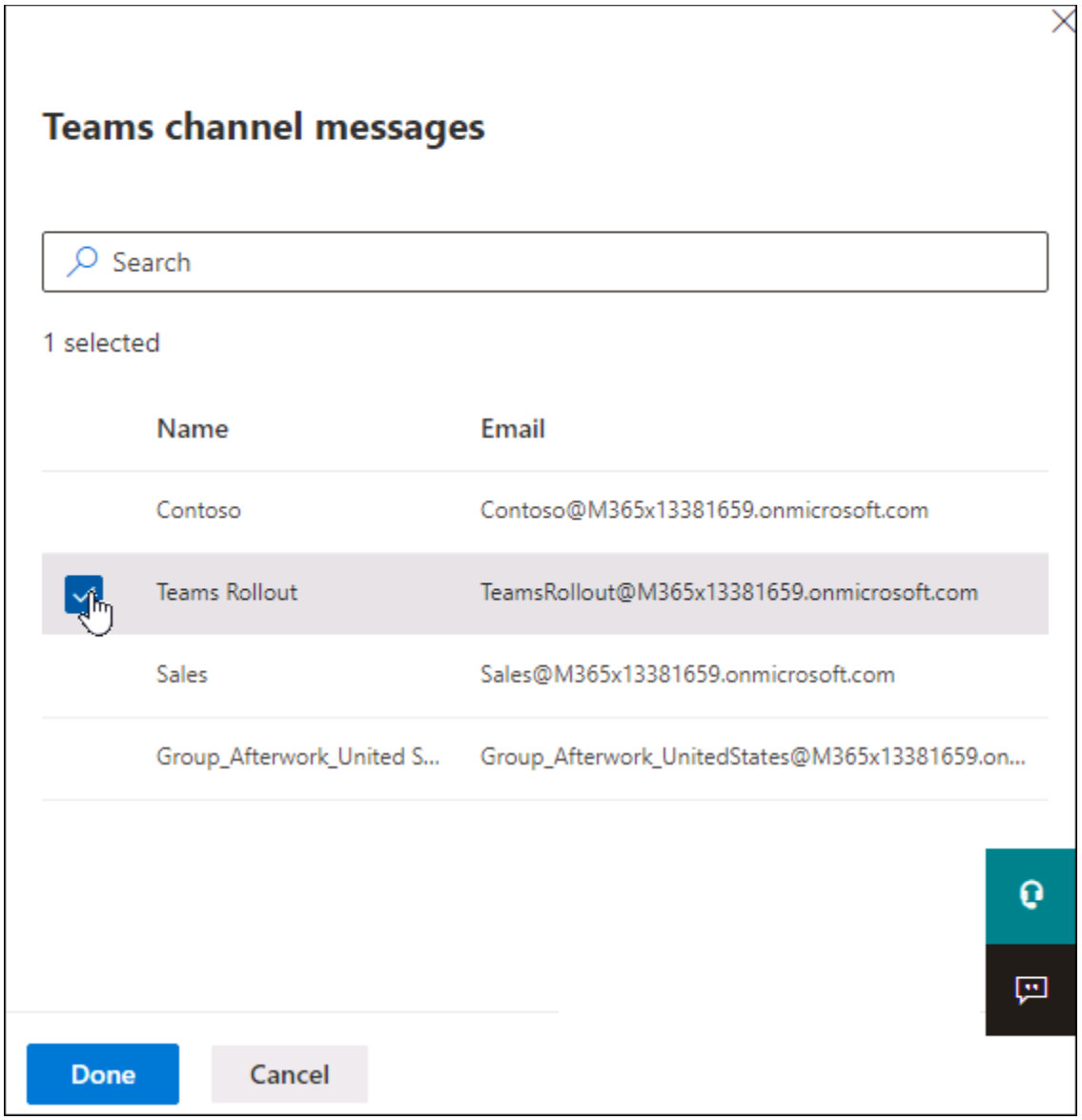
In this task, you have successfully created a new retention policy named **Sales retention policy** that retains the channel messages and chat of the **Sales** Team for **7 years after the last modification**.

Task 5 - Create a new retention policy to delete content

After configuring a retention policy to protect data from deletion, you also need to evaluate the capabilities of retention policies to delete content automatically. For demonstration purposes, you will set the deletion threshold to a single day and apply the retention policy to the **Teams Rollout** team, to remove all channel messages older than a day automatically.

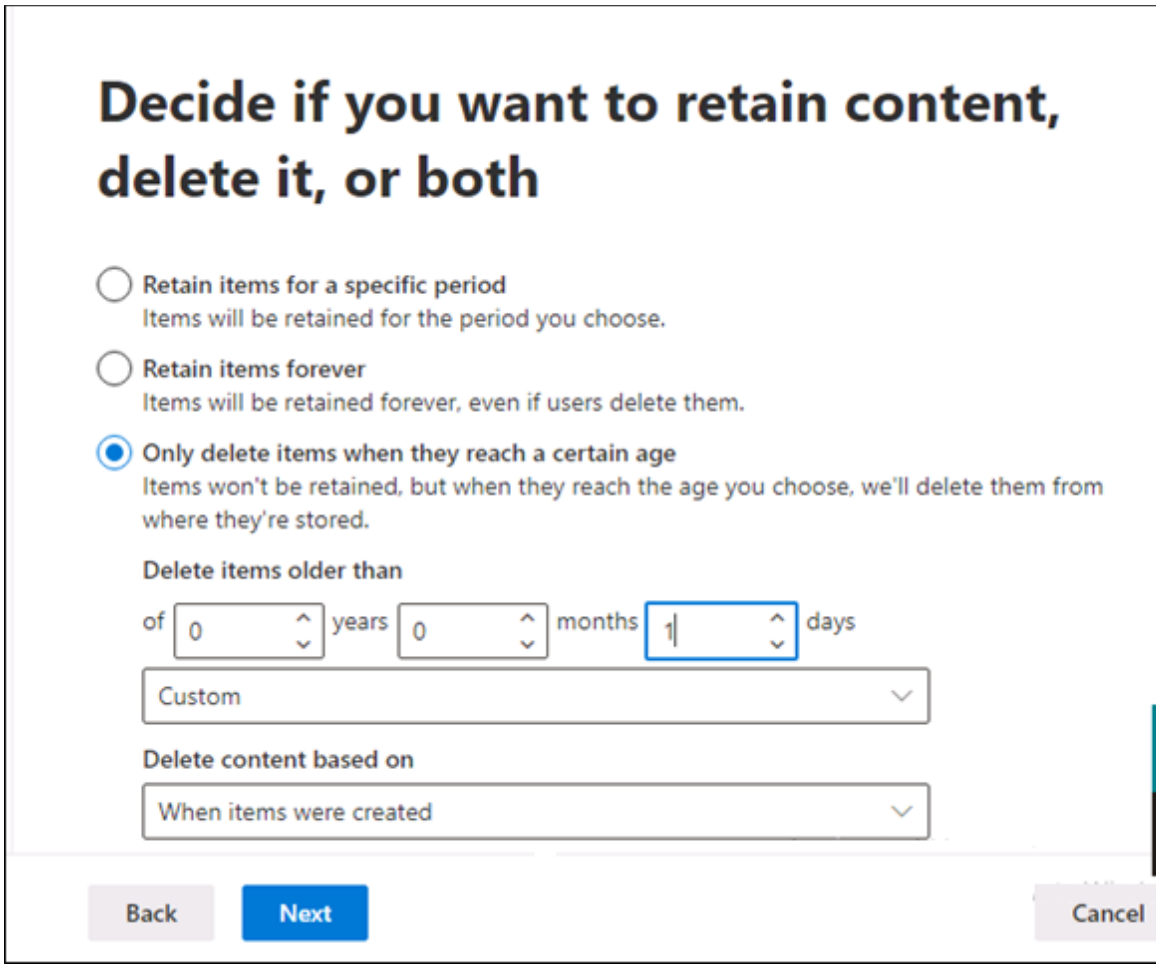
1. Browse to Microsoft Purview Portal (https://compliance.microsoft.com/).
2. In the left navigation of the Microsoft Purview Portal, select **Data lifecycle management**. From the drop down select **Microsoft 365**.
3. On the **Data lifecycle management** page, under **Retention** policies tab, select +New retention policy to add new Retention Policy.
4. Follow the **Create retention policy** wizard with the following information:
    i. In the **Name** section, enter the following information
        - **Name**: Teams Rollout deletion policy
        - **Description**: Retention policy for the Teams Rollout team to delete messages older than a day.
        - Select **Next**
    ii. In the **Type** section,select **Static** and select **Next** then configure the following settings:
        - **Exchange email**: Off
        - **SharePoint sites**: Off
        - **OneDrive accounts**: Off
        - **Microsoft 365 Groups**: Off
        - **Skype for Business**: Off

- **Exchange public folders**: Off
- **Teams channel messages**: On
- **Teams chats**: Off
- **Teams private channel messages**: Off
- **Yammer community message**: Off
- **Yammer user messages**: Off
- Select **Edit** in the **Included** column (under the current *All teams* choice) for the **Teams channel messages** line to open the right-side pane.
- Select the checkbox left from **Teams Rollout** and select **Done**.



iii. In the **Retention settings** section,

- Select **Only delete items when they reach a certain age**
- Delete items older than: Select **Custom** > **1 days**
- Delete the content based on: **when items were created**
- Select **Next**.



5. In the **Finish** section, review your settings and select **Submit**.

6. Select **Done**. Leave the browser open for the next task.

You have successfully created a second retention policy for testing the deletion capabilities to clean up the **Teams Rollout** team from all conversation messages older than a day.

Task 6 – Test the retention policy for deleting content (optional)

In this task, you will test the retention policy for deleting content from the **Teams Rollout** team after a day. Before you can see the retention policy taking any effect, you must create some conversation content in the team.

Note: Because you need to wait for 24 hours till the retention policy deletes anything, this task is marked as optional. After creating content in the Teams Rollout team, you need to return to this task after waiting 24 hours to see the retention policy's effect.

1. Open the Teams where you are still signed in.
2. Select the **Teams Rollout** team and the **General** channel.
3. Select **New conversation** from the lower end of the main window.
4. Write the following text to the text box:

- Hello world!

6. Leave the client open and add other content to the team, as you like.
7. Come back after 24 hours to see, the content has been deleted automatically.

You have added a conversation message to a team, which is deleted by the deletion retention policy after 24 hours.

Task 7 - Create a DLP policy for GDPR (PII) content from a template

According to your organization's compliance requirements, you need to implement basic protection of PII data for European users. You will create a new DLP Policy named **GDPR DLP Policy** from the template "General Data Protection Regulation (GDPR)," The DLP policy you create will detect if GDPR sensitive content is shared with people outside of your organization. If the policy detects at least one occurrence of the GDPR sensitive information, it will send an email to the **Teams admin - Joni Sherman** and block people from sharing the content and restricting access to shared content. Furthermore, it will display a tip to users who tried to share the sensitive content, and it will allow them to override the policy with business justification. Since you are evaluating the DLP policies, you will create the DLP policy in a test mode with policy tips enabled.

1. Browse to Microsoft Purview Portal (https://compliance.microsoft.com/).
2. In the left navigation of the Microsoft Purview Portal, select **Data loss prevention** under **Solutions**.
3. On the **Data loss prevention** page, select the **Policies** tab, then select **+ Create policy**.
4. In the **Choose the information to protect** section,

i. Select the **Search for specific templates** search box and type: **GDPR**.

ii. Select **Privacy** under **Categories**, then select the **General Data Protection Regulation (GDPR) Enhanced** template from the **Templates** section.

iii. Select **Next**

5. In the **Name your policy** section, enter the following information:
    - **Name**: GDPR DLP Policy
    - **Description**: Data loss prevention policy for GDPR regulations in Teams.
6. In the **Locations to apply the policy** section, apply the following settings and select **Next**:
    - **Exchange email**: On
    - **SharePoint sites**: On
    - **OneDrive accounts**: On
    - **Teams chat and channel messages**: On
    - **Microsoft Defender for Cloud Apps**: On
7. In the **Policy settings** section, stay with the default selection from the template - **Review and customize default settings from the template** and select **Next**.

    i. In the **Info to protect** section, leave the default settings and select **Next**.

    ii. In the **Protection actions** section, ensure that the following settings are configured, and then select **Next**:

        - A checkbox is selected for: **Detect when a specific amount of sensitive info is being shared at one time**
        - In the **At least __ or more instances of the same sensitive info type** box, type: **1**
        - Select the checkbox **Send incident reports in email**
        - Select **Choose what to include in the report and who receives it** to open the right-side pane
        - Select **Add or remove people**, select the checkbox for **Joni Sherman**.

- Select **Add** and **Save**
- Select the checkbox **Send alerts if any of the DLP rules match**
- Select the checkbox **Restrict access or encrypt the content in Microsoft 365 locations**

iii. In the **Customize access and override settings** section, ensure that the following settings are configured, and then select **Next**:

- A checkbox is selected for: **Restrict access or encrypt the content in Microsoft 365 locations**
- Select **Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams content**.
- Select **Block only people outside your organization.**.
- Select **Override the rule automatically if they report it as false positive**.

8. In the **Test or turn on the policy** section, select **Turn it on right away** and select **Next**.
9. On the Review your settings page, review your settings, select **Submit** then **Done**.
10. Stay on the **Data loss prevention page** and leave the browser opened.

After completing this task, you have created a DLP Policy from the template "General Data Protection Regulation (GDPR)" that detects if GDPR sensitive content is shared with people outside of your organization. The policy is extra sensitive for the configured threshold of **1** rule match and **Joni Sherman** will be notified if a matching occurs.

Task 8 - Create a DLP policy from scratch

After creating a DLP Policy for protecting GDPR relevant data, you will create another policy from scratch. Instead of using a template, you will configure rules directly with custom rules and actions.

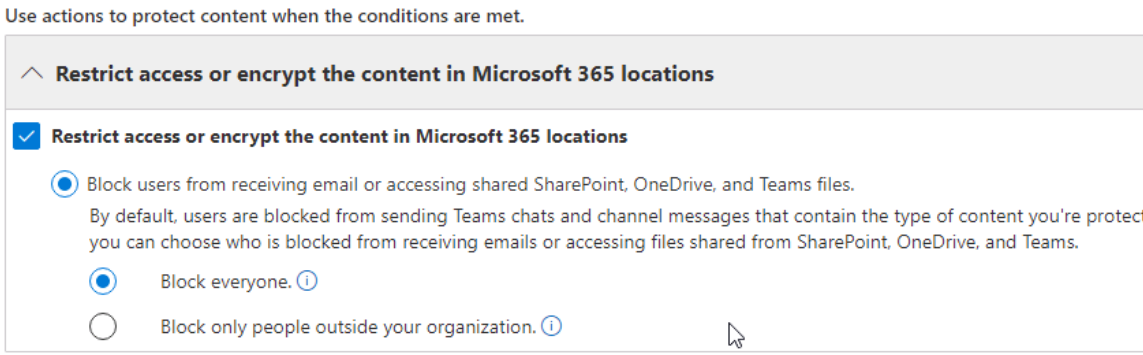
1. Browse to Microsoft Purview Portal (https://compliance.microsoft.com/).
2. In left navigation of the Microsoft Purview Portal, select **Data loss prevention** under **Solutions**.

3. On the **Data loss prevention** page, select the **Policies** tab, then select **+ Create policy**.
4. In the **Choose the information to protect** section,
    i. Select **Custom** under **Categories**, then select the **Custom policy** template from the **Templates** section.
    ii. Select **Next**
5. In the **Name your policy** section, enter the following information:
    - **Name**: Credit card data DLP Policy
    - **Description**: Data loss prevention policy for credit card data in Teams.
6. In the **Locations to apply the policy** section, apply the following settings and select **Next**:
    - **Exchange email**: On
    - **SharePoint sites**: On
    - **OneDrive accounts**: On
    - **Teams chat and channel messages**: On
    - **Microsoft Defender for Cloud Apps**: On
    - **On-premises repositories**: Off
    - **Power BI**: Off
7. In the **Policy settings** section, stay with the default selection and select **Next**.
    i. In the **Customize Advanced DLP rules** section, select **+ Create rule** and enter the following information:
        - **Name**: Credit card numbers found
        - **Description**: Basic rule for protecting credit card numbers forms being shared in Teams.
    ii. Below **Conditions**,
        - Select **+ Add condition** and **Content contains**.

- Leave the group name of **Default**, select **Add** and **Sensitive info types**.
- From the right-side pane, check the box left of **Credit Card Number** and select **Add**.
- Leave the high **High confidence** and **Instance count (1)** unchanged.

iii. Below **Action**,

- Select **+ Add an action** and **Restrict access or encrypt the content in Microsoft 365 locations**.
- Select the checkbox of **Restrict access or encrypt the content in Microsoft 365 locations** again and select **Block everyone**



iv. Below **User notification**,

- Select the slider to **On**
- Select **Notify the user who sent, shared or last modified the content**.
- Select **Customize the policy tip text**.

- Enter the following text to the textbox: **Credit card numbers are not allowed to be shared!**

v. Below **Incident reports**,

- Set the slider **Send an alert to admins when a rule match occurs** to **Off**.
- Select **Save**.

vi. Review the rule settings and select **Next**.

8. In the **Test or turn on the policy** section, select **Turn it on right away** and select **Next**.

9. On the Review your settings page, review your settings, select **Submit** then **Done**.

10. Leave the browser open.

You have successfully created a new custom DLP policy for protecting credit card numbers from being shared via Teams conversations.

Task 9 – Test the DLP Policies

To make sure your configured DLP policies are working as expected, you need to perform some testing with your pilot users.

Note: It can take up to 24 hours till new DLP policies take effect. If the step doesn't work, continue with the lab, and perform a task at a later point of working through this lab.

1. Open the Teams, where you are still signed in.

2. In the left-hand navigation pane, select **Teams**, and then select the **General** channel below **Teams Rollout**.

3. Select **New conversation** from the main window.

4. Enter the following lines to the textbox:

   - MasterCard: 5105105105105100

   - Visa: 4111111111111111

- Visa: 4012888888881881

5. Select the arrow to the right from the lower-right corner below the text box to send the message.

6. After a moment, you should see a text in red above your new conversation message that states, "**This message was blocked.**" **Select What can I do?** To see the reason why this message was blocked.

7. Select **Report** to notify the admin about this DLP policy violation. Now you can see a different message above your conversation entry, that states **Blocked. You've reported this to your admin.**

8. You should still be logged in to the **Microsoft Purview Portal**. If not, open Microsoft Edge, maximize the browser, and navigate to the **Microsoft Purview Portal**: **https://compliance.microsoft.com**.

9. Select **Reports** from the left-hand navigation pane and scroll down to **Organizational data**.

10. Below **DLP Policy Matches** and **DLP Incidents**, you can now see the DLP policy matches. Select **DLP Policy Matches** to open the detailed view.

11. On the **DLP Policy Matches** page, inspect the rule matches.

You have successfully tested your DLP policy to block sharing of credit card information via Teams chat and channel conversations.

Exercise 3: Prepare network deployment

Microsoft Teams provides users with chat, audio, video, and content sharing experience in different network conditions. It includes variable codecs, where media can be negotiated in limited bandwidth environments. However, as a Teams admin, you will need to carefully plan your network bandwidth, because there are other Office 365 services and third-party apps that also need a reliable network connection. Therefore, Teams admins must-have tools that could help to estimate the bandwidth consumption according to specific business requirements and existing network infrastructure and provide the best experience to business users.

Task 1 - Calculate network bandwidth capacity

In this exercise, you will calculate the network requirements for Microsoft teams, depending on your expected Teams usage business requirements. You must ensure enough bandwidth based on your organization network connectivity that is described in the following table (this is just an example):

Location	Total number of employees	WAN link capacity / audio/video queue size (Mbps)	Office 365 connection	Internet connection
New York HQ	1000 (100 Specialized calling only employees)	1000/300/500	ExpressRoute	Local Internet 1000 Mbps
Los Angeles Office	250 (50 Specialized calling only employees)	500/100/200	Remote connection through HQ	Remote Internet through HQ
Houston Office	150 (50 Specialized calling only employees)	400/50/100	Remote connection through HQ	Remote Internet through HQ

Next, you will analyze your current bandwidth usage and test your network quality and connection to Microsoft Teams. You will also need to troubleshoot potential voice quality issues.

1. Sign in to the **Teams admin center** (**https://admin.teams.microsoft.com**) (youruser@<YourTenant>.onmicrosoft.com).

2. Create a network plan

i. On the left-hand navigation pane, expand **Planning**, and select **Network Planner**.

ii. On the **Network planner** page, under **Network plans** tab, select **Add** and create a network plan with the following information.

- Network plan name: **Your Corporation plan**
- Description: **Your Corporation Network plan**
- Select **Apply**.

3. Create a custom personas

i. On the **Network planner** page, select **Personas** tab, and then select **+ Add**.

ii. On the **Add persona** page, create a custom personas with the following information.

- Persona name: **Calling only**
- Description: **Specialized calling only employees**
- Permissions: Turn on **Audio**
- Select **Apply**.

iii. Note the default personas recommended by Microsoft.

4. Create network sites.

i. Select the **Networks plans** tab, then select **Your Corporation plan**.

ii. Under **Network sites** tab, select **+ Add network site**.

iii. Create a network site for **New York HQ** with the following information.

- Network site name: **New York HQ site**
- Description: **New York HQ site network infrastructure**
- Network users: **1000**
- Network settings - Subnet: **172.16.0.0**
- Network settings - Network range: **16**
- Turn **On** the **Express Route** button.
- Internet link capacity: **1000**
- PSTN egress: choose **Use VoIP only**

- Select **Save**.

iv. Repeat the same steps to create a network site for **Los Angeles office** with the following information.

- Network site name: **Los Angeles site**
- Description: **Los Angeles site network infrastructure**
- Network users: **250**
- Network settings - Subnet: **192.168.10.0**
- Network settings - Network range: **24**
- Ensure **Express Route** button is **Off**.
- Turn **On** the **Connected to WAN** button.
- WAN link capacity: **500**
- WAN audio queue size: **100**
- WAN video queue size: **200**
- PSTN egress: choose **Use VoIP only**
- Select **Save**.

v. Repeat the same steps to create a network site for **Houston office** with the following information.

- Network site name: **Houston site**
- Description: **Houston site network infrastructure**
- Network users: **150**
- Network settings - Subnet: **192.168.20.0**
- Network settings - Network range: **24**
- Ensure **Express Route** button is **Off**.
- Turn **On** the **Connected to WAN** button.
- WAN link capacity: **400**
- WAN audio queue size: **50**
- WAN video queue size: **100**
- PSTN egress: choose **Use VoIP only**
- Select **Save**.

5. Create a report

i. On the **Your organization plan** page, select **Report** tab and then select **+ Add report**.

ii. Create a report with the following information.

- Report name: **Your organization report**
- Description: **Your organization network estimation report**
- Under the **Calculation** section, specify the **Persona** and **Network users** with the following information.

Network site	Persona and Network users
New York HQ	Office Worker: 900 Calling only: 100
Los Angeles Office	Office Worker: 200 Calling only: 50
Houston Office	Office Worker: 100 Calling only: 50

iii. Select **Generate report**.

6. Under the **Reports** section, review the impact of Microsoft Teams on the Your organization network infrastructure by analyzing the report results on bandwidth needed for audio, video, screen sharing, Microsoft 365 traffic, and PSTN.

7. On the report page, select the **Chart view** at the upper-right hand corner to display report results in different views.

Once you generate the report, you'll see the recommendation of your bandwidth requirements. The allowed bandwidth shows how much of your overall traffic is reserved for real-time communications. Thirty percent is the recommended threshold. By changing this value and selecting **Run report**, you can see the different impacts on the bandwidth for your network. Any areas that need more bandwidth will be highlighted in

red. Work with your instructor to modify the parameters in the Network Planner and verify different results based on the input data.

In this lab, you have used Network Planner to estimate the Microsoft Teams impact on the bandwidth in your network infrastructure.

Task 2 - Use Microsoft 365 network connectivity test tool

You are in the planning phase of a Microsoft Teams deployment. Before deploying Microsoft Teams in your organization, you want to test your network quality and connection to Microsoft Teams. After completing the test, you will interpret the results and gain insights into potential network issues.

1. Browse to the Microsoft 365 network connectivity test tool(https://connectivity.office.com).

2. Select **Sign in** at the top-right corner.

3. Specify the location and select **Run test**.

   You can type in your location by city, state, and country or you can have it detected from the web browser.

4. Select **Open file** when prompted after downloading the advanced client test application.

   Note: The application requires .NET Core installed. Select **Yes** if you get prompted to install .NET Core. Select **Download x64** under **Run desktop apps** section then follow the installation instruction.

5. Start the advanced tests client application - **Office 365 Network Onboarding Advanced Tests**.

   - Download the application
   - Navigate to downloads folder and run the client application

6. Once the client application starts, the web page will update to show this result.

7. Review the result under **Details** tab.

In this task, you have used Microsoft 365 network connectivity test tool to test the connectivity and connection quality of your network infrastructure for Microsoft Teams.

Lab 03: Manage teams, collaboration and app settings for Teams

Student lab answer key

Lab Scenario

In the labs of this course, you will assume the role, a Teams Administrator for your corporation. In this lab, you will perform operational tasks as a Teams administrator, such as creating and modifying teams, managing membership, and recovering deleted teams.

In managing collaboration in Microsoft Teams, you will manage chat and collaboration experiences such as team settings or private channel creation policies. Finally, you will manage settings for Teams apps such as app permission and app setup policies, Apps, bots & connectors in Microsoft Teams or publish a custom app in Microsoft Teams.

Objectives

After you complete this lab, you will be able to:

- Create a Team from a Microsoft 365 Group
- Create a Team by using Microsoft Graph API
- Create a Team with dynamic membership
- Archive and unarchive Teams
- Delete and recover Teams
- Create a messaging policy
- Manage private channels
- Disable third-party storage providers
- Manage Policy packages

- Edit and test default org-wide app policy
- Edit and test default app permission policy
- Create and manage a custom app setup policy

Lab Setup

- **Estimated Time:** 110 minutes.

Instructions

Exercise 1: Manage team resources

Task 1 - Create a team from an existing Microsoft 365 group

As part of your pilot project for Your organization, you need to modify the **IT-Department** Microsoft 365 group, created in an earlier lab, and add Teams features to it.

1. Select the **Teams** icon on the taskbar to start the Teams desktop client and sign in as your user (youruser@<YourTenant>.OnMicrosoft.com).
2. The Microsoft Teams desktop client will start. If a **Bring your team together**, or **Get the Teams mobile app** window appears, close both windows.
3. In the left-hand navigation pane, select **Teams**, select **Join or create a team**, and then select **Create team** from the middle of the window.
4. In the **Create a team** dialog, select **From a group or team**.
5. In the **Create a new team from something you already own** dialog, select **Microsoft 365 group**.
6. In the **Which Microsoft 365 group do you want to use?** dialog, select the group **"IT-Department"**, then select **Create**. Wait until the **Creating the team…** process is done.
7. Select the three dots (**…**) right from the new team in the left pane and select **Manage team**.

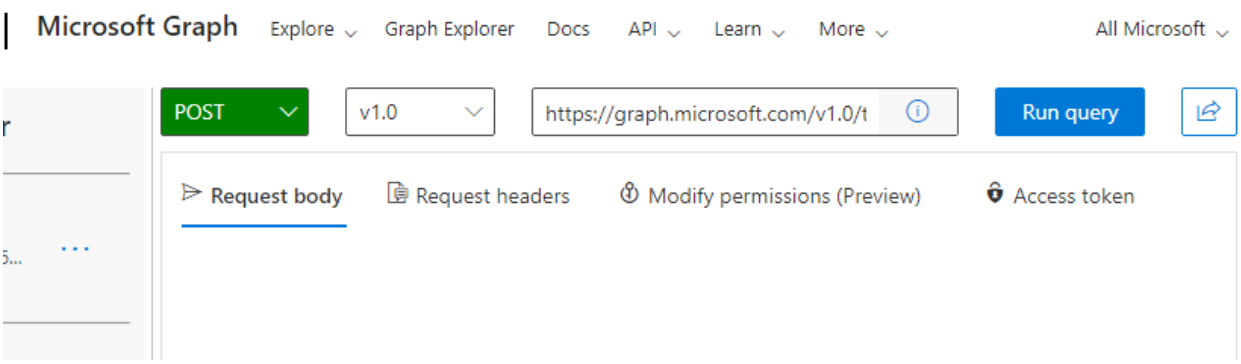
8. Check the team owner and members:
    - Owners: **Joni Sherman**
    - Members and guests: **Allan Deyoung** , and **Patti Fernandezr**
9. Leave the Teams desktop client open and continue to the next task.

You have successfully created a new team with the Teams desktop client, by using an existing Microsoft 365 group. Leave the Teams client open and continue with the next task.

Task 2 - Create a team by using Graph API

In this task, you will test the Graph API capabilities for certain automation plans of your organization with Teams. For this task, you will create a new team, called **Early Adopters** with minimal settings, such as Public join options, and another team with multiple existing channels, called **Tech Meetings**.

1. Open Microsoft Edge, maximize the browser, and navigate to the **Graph Explorer** at: https://developer.microsoft.com/graph/graph-explorer
2. Select the **Sign in to Graph Explorer** button in the left of the page and sign in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. If you access the Graph Explorer for the first time, you will see a **Permissions requested** page. Select **Accept**.
4. Select the **GET** button and select **POST** from the dropdown menu.
5. Do not change the **v1.0** from the box in the middle.
6. Enter the following to the text box before the **Run query** button:
    - https://graph.microsoft.com/v1.0/teams
7. Select **Modify permissions (Preview)** from the top pane.



8. Scroll to the right and select the **Consent** button for the permissions **Team.Create**.

9. Another **Permissions requested** page appears. Select **Accept**.

10. If you are redirected to the Microsoft Developers site, navigate back to the **Graph Explorer** at: https://developer.microsoft.com/graph/graph-explorer

11. Select the **Request body** tab and enter the following code:

```
12. {
13.
14. "template@odata.bind":"https://graph.microsoft.com/v1.0/teamsTemplates('standa
    rd')",
15.
16. "displayName": "Early Adopters",
17.
18. "description": "The Early Adopters Workspace.",
19.
20. "visibility": "Public"
21.
    }
```

22. Select **Run query** from the upper right of the page.

23. After a moment, you should see a green bar below the Request body window, with a checkmark and an **Accepted** message.

24. Remove the whole content of the textbox in the textbox of **Request body**, you just used to create a team and replace it with the following content:

```
25. {
26.
27. "template@odata.bind":
    "https://graph.microsoft.com/v1.0/teamsTemplates('standard')",
28.
29. "visibility": "Public",
30.
```

```
"displayName": "Tech Meetings",

"description": "Space for all employees participating in the champions program, who want exchange each other about the newest features.",

"channels": [

{

"displayName": "Welcome Hall",

"isFavoriteByDefault": true,

"description": "Channel for introducing yourself as a member of the tech meeting participants."

},

{

"displayName": "Tech Lunch and Dinner",

"isFavoriteByDefault": true,

"description": "When will be the next tech lunch and who has any suggestions where to meet."

},

{

"displayName": "Q and A",

"description": "Questions and answers: Teams users giving a helping hand to other users.",

"isFavoriteByDefault": true

},

{

"displayName": "Issues and Feedback 🏵",

"description": "Leave some feedback for the IT-Staff.",

"isFavoriteByDefault": false

}

],

"memberSettings": {

"allowCreateUpdateChannels": true,
```

```
82.
83. "allowDeleteChannels": false,
84.
85. "allowAddRemoveApps": true,
86.
87. "allowCreateUpdateRemoveTabs": true,
88.
89. "allowCreateUpdateRemoveConnectors": true
90.
91. },
92.
93. "guestSettings": {
94.
95. "allowCreateUpdateChannels": true,
96.
97. "allowDeleteChannels": false
98.
99. },
100.
101. "funSettings": {
102.
103. "allowGiphy": true,
104.
105. "giphyContentRating": "Moderate",
106.
107. "allowStickersAndMemes": true,
108.
109. "allowCustomMemes": true
110.
111. },
112.
113. "messagingSettings": {
114.
115. "allowUserEditMessages": true,
116.
117. "allowUserDeleteMessages": true,
118.
119. "allowOwnerDeleteMessages": true,
120.
121. "allowTeamMentions": true,
122.
123. "allowChannelMentions": true
124.
125. },
126.
127. "discoverySettings": {
128.
129. "showInTeamsSearchAndSuggestions": true
130.
131. }
132.
   }
```

133. Select **Run query** from the upper right of the page.

134. After a moment, you should see a green bar with a checkmark and **Accepted** inside again.

135. Open the Teams Desktop App. Select **Teams** and manage teams from the left-side pane and inspect the newly created teams "**Early Adopters"** and"**Tech Meetings**".

You have successfully created two teams via Graph API. Your test of the Graph functionality is complete, and you can advance to the next exercise.

Task 3 – Archive and unarchive a team

After creating the different teams in this lab, you also need to evaluate the different ways of removing teams again. In this task, you will test the archiving function and change the Sales team to a non-activate state without deleting its content. This function is required for some company's compliance requirements of retaining the stored data inside the teams. The only Teams administrative role with sufficient privilege for this task is the Teams Administrator, which is currently assigned to Joni Sherman, therefore you will use Joni's account for this task.

1. Browse to the **Teams admin center**: https://admin.teams.microsoft.com
2. Sign in with youruser@<YourTenant>.onmicrosoft.com).
3. Select **Teams** from the left-side pane and **Manage teams**.
4. Archive the **Sales** team
    i. Select the checkmark left from the **Sales** team and select **Archive** from the top pane.
    ii. Select the checkbox of **Make the SharePoint site read-only for team members** and select **Archive**.
    iii. The **Status** column should now have changed to **Archived**, written in orange color. Leave the browser open and proceed. If you have problems with the **Sales** team - archive another team (you can undo this action in the unarchive step).
5. Check the archived team

i. Browse to the **Microsoft Teams web client (https://teams.microsoft.com/)** as **youruser**@<YourTenant>.onmicrosoft.com).

ii. Select Teams and then select the gear icon(Manage Teams) next to **Join or create a team.**

iii. Expand **Archived** section, and select **Sales** team. You can see the **Sales** team under the **Hidden teams** section.

iv. Select **General** channel under the **Sales** team, notice the **New conversation** option is not available.

6. Unarchive the **Sales** team

   i. Browse to the Teams admin center.

   ii. Select the checkbox left from **Sales** again and select **Unarchive** from the top menu. The **Status** field should change to **Active** again.

7. Check the unarchived team

   i. Browse to the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).

   ii. On the left side, select **Teams**.

   iii. Notice that the text of the **Sales** team and the **General** channel changes back to normal after a moment, but the team is hidden.

   iv. Select the three dots (...) right from the Sales team and select **Show**.

8. Leave the browser open and stay signed in.

You have successfully archived a team and reviewed the limited functionality of archived teams. This fulfills the first requirement of testing the archiving function of teams for compliance preservation policies and rules. After this test, you have unarchived the team again, making it fully operational again.

Task 4 - Delete and recover teams

In this task, you will delete one of the teams created in the previous lesson and learn how to restore it.

1. Browse to the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).

2. In the left-hand navigation pane of the Teams web client, select the three dots (...) right from the **Sales** team and select **Delete the team** from the list.

3. In the **Delete the Sales team**, select **I understand that everything will be deleted**. and select **Delete team**.

4. Restore group

    i. Browse to Azure AD admin center (https://aad.portal.azure.com/).

    ii. On the left navigation pane, select **Azure Active Directory** > **Groups**.

    iii. On the **Groups | All groups** page, select **Deleted groups** in the left side pane.

    iv. Now you can see all deleted groups, including the **Sales** group.

    v. Select the checkbox left from the **Sales** group and select **Restore group** from the top pane. Confirm the **Do you want to restore deleted groups dialog** by selecting **Yes**.

5. Check the restored group.

    i. Browse to the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).

    ii. The **Sales** team appears in the list of teams again. Press **F5** to refresh the page if needed.

    iii. Select the three dots (...) right from the team name and select **Manage team**. You can see the owner and all members again in the **Members** tab.

Note: The full process of deleting and restoring a team can take up to 24 hours. If it does not appear again, check for it at a later point in this lab.

You have successfully deleted a team via the Teams web client and restored it with the Azure Portal.

Task 5 - Manage team members with dynamic membership

Your organization is expanding to Canada and will open a new office in Toronto. As a system administrator, you need to configure a dynamic group with membership based on the location of the Office 365 services.

1. Browse to Azure AD admin center (https://aad.portal.azure.com/).
2. On the left navigation pane, select **Azure Active Directory** > **Groups**.
3. On the **Groups | All groups** page, search and select **CA-Office** group.
4. On the **CA-Office** page, select **Properties** from the left-hand navigation pane.
5. Change the **Membership type** from **Assigned** to **Dynamic User**.
6. Select **Add dynamic query** below **Dynamic user members**.
7. On the **Dynamic membership rules** page, enter the following information to the fields:
    - Property: **accountEnabled**
    - Operator: **Equals**
    - Value: **true**
8. Select **+add expression** and enter the following information to the fields:
    - Property: **usageLocation**
    - Operator: **Equals**
    - Value: **CA**
9. Select **Save** twice.

    A warning message is displayed, that the membership will change according to the new dynamic membership rules. Select **Yes** to confirm the message.
10. Select **Overview** in the left-hand navigation pane of the **CA-Office** group window.
11. In the Overview window, locate **Dynamic rule processing status** field.

Wait and refresh your browser, until the status says **Update complete**. It may take several minutes for the change to be processed.

12. Then select **Members** in the left-hand navigation pane and then select **Refresh**. Verify that **Alex Wilber** is in the list of members, but that **Allan Deyoung** has been removed from the group.

13. Select Owners from the left-hand navigation pane and verify, that Joni is still the Owner of the group, even if she does not match the dynamic group criteria.

You have successfully converted a Microsoft 365 group from static (assigned) to dynamic membership. This membership is controlled by the usageLocation of the user and if the account is enabled. Any user with the usageLocation "Canada" is added automatically to the team.

Exercise 2: Configure channel and message policies

In this exercise, you will configure policies to manage the creation of new private channels and the available tools for users in chat.

Task 1 - Create a messaging policy for giphy, memes, and stickers

The company wants to restrict the use of graphic elements in Teams communication. As a Teams service administrator, you will create a new message policy that prohibits pilot users from using GIF files, memes, and stickers in the Teams chat and channel conversation.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).

2. In the left navigation of the Teams admin center, select **Messaging policies**.

3. Select **+Add** under **Manage Policies** tab and enter the following

    - **Name**: Regular users without fun stuff
    - **Description**: Policy to disable giphys, stickers, and memes in conversations
    - **Giphys in conversations**: Off
    - **Memes in conversations**: Off
    - **Stickers in conversations**: Off

- Leave the rest of the settings as default. Select **Save**.

4. Back to the **Messaging policies** overview page, select the checkmark left to **Regular users without fun stuff**. Then select **Assign users**

   Note: If you didn't see **Assign users**, select … to expand the menu.

5. Search and select **add** for the following pilot users. Then select **Apply**.

   - **Alex Wilber**
   - **Lynne Robbins**
   - **Diego Siciliani**

Note: It can take up to 24 hours for the settings to take effect.

In this task, you have successfully configured a new messaging policy and assigned it to the pilot users. It will now take some time for the policy to take effect. Continue with the next task.

Task 2 - Manage private channels in a team

As Teams administrator of Your organization, you will create a private channel named **confidential** in the sales team that is only accessible for some team members.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In left navigation of the Teams admin center, select **Teams** > **Manage teams**.
3. Select the **Sales** team > **Channels** tab.
4. Add the private channel

   i. Select **+ Add** from the top menu.

   ii. In the **Add** window, enter the following information:

   - **Name**: Confidential sales
   - **Description**: Confidential private sales channel
   - **Type**: Private

- **Channel owner**: Lynne Robbins

5. Select **Apply**.
6. Check the private channel
    i. Browse to the **Teams Web Client** (https://teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
    ii. Select **Teams**, you should see the new private channel **Confidential sales** with a small padlock icon.

In this task, you learned how to create a private channel in the Microsoft Teams admin center and how to configure and check the access.

Exercise 3: Manage app settings

Task 1 - Disable third-party storage providers

In the past, users stored data at various locations, including third-party storage providers. Recently, the company deployed OneDrive for all users and would like to guide the users to use SharePoint and OneDrive as the primary data storage locations with Box as an alternative for all file collaborations. As the Teams admin, you are asked to deactivate all third-party storage providers except Box in Microsoft Teams to align with the direction.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In left navigation of the Teams admin center, select **Teams** > **Teams settings**.
3. On the **Teams settings** page, go to the **Files** section.
4. Configure the following file sharing and cloud file storage options.
    - **Citrix files:** Off
    - **DropBox:** Off
    - **Box:** On
    - **Google Drive:** Off

- **Egnyte:** Off

5. Scroll down and select **Save**.

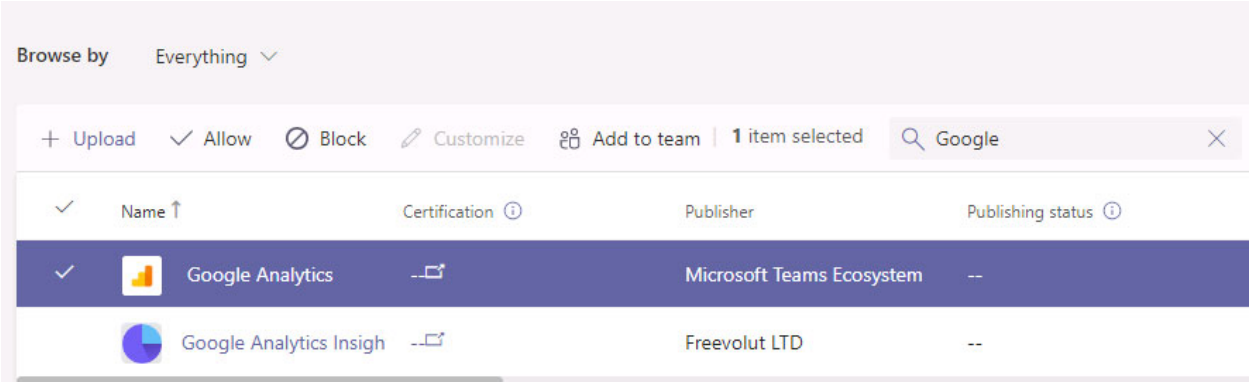
Note: It can take up to 24 hours for the settings to take effect.

In this task, you have learned how to enable or disable third-party storage providers for your whole tenant.

Task 2 - Block an app at organizational level

In this task, you will block the Google Analytics app for all tenants

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In the left navigation of the Teams admin center, select **Teams apps** > **Manage apps**.
3. On the **Manage apps** page, type **Google** in the search box.



4. In the search result, select **Google Analytics** to highlight the app.
5. Select **Block** from the top menu.
6. Select **Block** again from the prompt window to confirm the setting.

Note: It can take up to 24 hours for the settings to take effect.

In this task, you have learned how to block the Google Analytics app for your tenant.

Exercise 4: Create and manage app setup policies

As a Teams administrator you need to highlight the apps that are most important for your users and also showcase apps that users in your organization need, including apps built by third-parties or by parties or by developers in your organization.

Task 1 - Edit default org-wide app policy

In the pilot project, the company wants to add **Tasks by Planner and To Do** as the default app for all users. To do this, edit the default org-wide app policy. This task may take some time to propagate throughout the tenant.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In the left navigation of the Teams admin center, select **Teams apps** > **Setup policies**.
3. On the **App setup policies** page, Under **Manage Policies,** select on **Global (Org-wide default)** to open the org-wide app policy.
4. In the **Pinned apps** section, select **Add apps**.
5. From the **Add installed apps** page, select **Global** and search **Planner**. You will see **Tasks by Planner and To Do** app, mouseover the name and select **Add** twice.
6. Make sure that **Tasks by Planner and To Do** is now listed in the **Pinned apps** section then select **Save**.

Note: It can take up to 24 hours for the settings to take effect.

In this task, you learned how to pin default apps from the Microsoft Teams admin center.

Task 2 - Create a custom app setup policy

1. Browse to Teams admin center (**https://admin.teams.microsoft.com**) (**youruser@<YourTenant>.onmicrosoft.com**).
2. In the left navigation of the Microsoft Teams admin center, go to **Teams apps** > **Setup policies**.
3. Select **+ Add**.

4. Enter the following information
    - Name: **Sales team**
    - Description: **Install Adobe Acrobat Sign and pin Viva Goals**.
    - User pinning: **On**
    - To install apps for users:
        a. Under **Installed apps**, select **Add apps**.
        b. In the **Add installed apps** pane, search for the apps you want to automatically install for users when they start Teams.

            In this exercise search for **Adobe**, choose **Adobe Acrobat Sign** and select **Add** to add to the **Apps to add** list.

            You can now select **Add** to finish adding the app under **Installed apps list.**
    - To pin apps:
        a. Under **Pinned apps**, select **Add apps**.
        b. In the **Add pinned apps** pane, search for **Viva Goals** and then select **Add**.
        c. Select **Save.**
5. Select **Save.**

You have now created a new custom app set up policy.

Task 3 - Assign a custom app setup policy to users

1. In the left-hand navigation pane on the **Microsoft Teams admin center**, go to **Teams apps** > **Setup policies**.
2. Select **Sales team** app setup policy.
3. Select **Assign users**.
4. In the **Manage users** pane, search for **Alex Wilber**, and then select **Add**.

5. Select **Apply**.

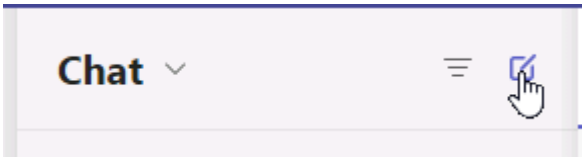
Exercise 5: Test configured policy settings

In this exercise, you will test the configured policy settings on a client with the affected user **Lynne Robbins** and compare the settings to the available client settings of **Joni Sherman**.

Task 1 – Test the messaging policy and private channel access

In this task, you will test the **messaging policies** configured in exercise 1 and compare the difference between an affected user (Lynne Robbins) vs a regular user(Joni Sherman).

1. Browse the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).
2. In the left-hand navigation pane, select **Chat** > **New Chat** icon.



3. In the main pane, enter **Joni Sherman** to start the conversation.
4. Notice there's no **giphy**, **memes** and **stickers** icons.

Task 2 – Test blocked app and storage providers

In this task, you will test the blocked app.

1. Browse the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).
2. In the left-hand navigation select **Apps**.
3. Search **Google** from the search box.
4. In the search results select **Google Analytics**. Note the lock icon and the "Request approval" button.

5. In the left-hand navigation pane, select **Teams**, go to the **General** channel of the **Sales** team.

6. Select the **files** tab and select **+ Add cloud storage** in the navigation pane below.

   Note: You can reload the tab or select … if you didn't see the option.

7. Notice that you only see SharePoint and Box as options, the cloud file storage settings in Teams settings worked as expected.

8. Sign out of Teams and close all open windows.

END OF LAB

Lab 04: - Manage Teams meetings and calling experiences

Student lab answer key

Lab Scenario

In the labs of this course, you will assume the role of Joni Sherman, a Teams Administrator for Your organization Ltd., and her pilot team that shall evaluate the capabilities of Microsoft Teams in a testing environment. Teams admins need to configure conferencing functionalities, such as meetings and live event features that will provide the best user experience during collaboration and communication.

Your organization is also planning to purchase and deploy multiple Team devices. You will need to evaluate different devices profiles and configure profile settings for the devices and the process of creating Microsoft Teams room, where multiple Teams' rooms will be purchased in your organization.

Furthermore, you will replace Your organization legacy PBX solution and configure voice features that will provide users with Teams calling capabilities.

Objectives

After you complete this lab, you will be able to:

- Manage meeting policies
- Configure meeting settings
- Create live event policies
- Create a webinar
- Create configuration profiles for devices
- Configure a new Microsoft Teams Room
- Set up a Calling Plan

- Order and Assign phone numbers
- Configure emergency addresses
- Create calling policies
- Configure resource accounts and calling queues
- Create resource accounts and auto attendants
- Access and navigate through call analytics ad CQD dashoards

Lab Setup

- **Estimated Time:** 180 minutes.

Instructions

Exercise 1: Manage Live event and meetings experiences

Your organization organization has deployed Microsoft 365 and is testing pilot projects on collaboration and communication scenarios to meet business requirements. The Teams admin will configure meeting policies and schedule an initial webinar for testing purposes.

Task 1 - Edit the default meeting policy and restrict all recording features for meetings

As part of your pilot project for setting up the events and meetings in your organization, you need to fulfill the requirement for all meetings in Teams, including prohibiting meeting recording. You will edit the default meeting policy to ensure that this requirement is met.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In left navigation of the Teams admin center, select **Meetings** > **Meeting policies**.
3. Select the **Global (Org-wide default)** policy under **Manage policies**.

4. On the **Meetings policies** page, turn **Off** the **Cloud recording** setting under the **Recording & transcription** section.

5. Select **Save**.

You have successfully modified the Global (Org-wide default) meeting policy and disabled the recording functionality for meetings. It will take some time for the changes to be applied to the users, so you will continue with the next task and test the configured settings at the end of this lab.

Task 2 – Test the meeting policy for restricting recording

In this task, you need to sign in to the second client and create a meeting with a user. You will see how the configured policy works and users won't be able to record a meeting.

1. Browse to the **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).

2. Select **Calendar** from the left navigation pane.

3. Select **Meet Now** > **Start meeting** from the upper right corner.

4. Select **Join now** to start the meeting.

5. Close **Invite people to join your window** by selecting **X** on the upper right corner.

6. In the meeting window, select … for **More actions**.

7. Notice that you can't select **Start recording**.

8. End the meeting.

Task 3 - Configure meeting settings and restrict anonymous users from joining meetings

Your company works with several external partners, and users often schedule meetings with external partners for projects collaboration. However, according to the company regulations, external partners need to identify themselves with a valid account, and anonymous access needs to be forbidden. You need to configure Microsoft Teams to disable anonymous access to meetings.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In left navigation of the Teams admin center, select **Meetings** > **Meetings settings**.
3. On the **Meetings settings** page, turn **Off** the option **Anonymous users can join a meeting** in the participants section.
4. Select **Save**.

You have successfully modified the meeting settings for all users in your tenant and disabled anonymous access to any meetings. It will take some time for the changes to be applied to the users, so you will continue with the next task and test the configured settings at the end of this lab.

Task 4 - Create a new live event policy and restrict recording capabilities

Your organization Ltd. wants to broadcast video and meeting content to large online audiences. As a Teams admin, you need to evaluate live events functionalities, including creating live events and configuring live event policies. According to your company Ltd. business requirements, you will need to restrict the recording options for participants of meetings and only allow recording options to manage users. Only the organizer of a live event should be able to record his meetings.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In the left navigation of the Teams admin center, select **Meetings** > **Live events policies**.
3. Select **+Add** under **Manage Policies** tab.
4. On the **Live events policies\Add** page, enter the following information:
    - Add live events policy Name: **Management Live Events**
    - Description: **Recording Restriction for live events organized by managers**
    - Live events scheduling: **On**
    - Transcription for attendees: **Off**

- Who can join scheduled live events: **Everyone in the organization**
- Who can record an event: **Organizer can record**

5. Select **Save**.
6. Back on the **Live events policies** page, select **Management Live Events** policy and under **Manage Users** select **Assign users** from the top menu.
7. In the **Manage users** pane, search and add **Lynne Robbins**.
8. Select **Apply** to assign the policy to the selected user.

You have successfully created a custom Live event policy and assigned it to a user.

Task 5 – Create a webinar

The IT department wants to host a company-wide meeting to answer employees' questions regarding the new reporting system. As a Teams admin, you will create a webinar allowing employees to submit their questions before the meeting.

1. Browse to **Microsoft Teams web client (https://teams.microsoft.com/)** (youruser@<YourTenant>.onmicrosoft.com).
2. In the Teams Calendar, select the dropdown menu **New meeting** and select **Webinar**. Scheduling page will open **Teams.Microsoft.com/Scheduling**.
3. Create a new **webinar**:
    - **Title**: IT Office Hours
    - **Start/End**: Select a time close to your current time
    - **Presenters**: Patti Fernandez, Allan Deyoung
4. Select **View registration form**, it opens a new webpage with the url **Teams.microsoft.com/registration**. Enter the following information:
    i. **Title**: IT Office Hours
    ii. Select **+ Add field** > **Custom question** > **Input**.
    iii. Enter the following to the textbox below **Custom question**:

    What is your question about the new reporting system?

iv. **Start/End**: Select a time close to your current time

v. Select **Save** and select **Copy registration link**. Preview the invitation by clicking the **View in browser** and closing the page.

vi. Go back to the **Teams.Microsoft.com/scheduling** window and click **Send** button to activate the Webinar registration.

vii. Click **Teams** on the left navigation pane, Select **General** under the **IT-Department**. Click the **New Conversation** and paste the copied registration link in the new conversation text box and click send.

viii. Sign out and close all browser windows.

5. Test the meeting registration.

   i. Browse to **Microsoft Teams web client (https://teams.microsoft.com/)** .

   ii. Go to the **General** channel of the **IT Department** team and select the registration link that you posted.

   iii. Fill out the registration form using <Your outlook account> and select **Register now**.

   iv. Go to **Outlook Web Portal** (https://outlook.live.com/owa/), and check the email with subject **You're registered for IT Office Hours**

   v. Sign out and close all browser windows.

You have successfully created a webinar with a custom registration form.

Exercise 2: Deploy Teams device profiles

As a Teams administrator, you will create configuration profiles to manage settings and features for Teams devices in your organization. You can create or upload configuration profiles to include settings and features you want to enable or disable and then assign a profile to a device or groups of devices.

Your organization could purchase Microsoft Teams Rooms that provide a complete meeting experience with HD video, audio, and content sharing in conference rooms. You will need to prepare the deployment prerequisites by defining Microsoft Teams Rooms service account in Office 365.

Task 1 - Create configuration profiles

During the planning phase of Teams Phones devices in your organization, you want to evaluate settings that can be applied to Teams devices by using configuration profiles in Teams admin center. You will create a configuration profile for Teams device and analyze settings that will include in the configuration profile. Once devices are deployed into your organization, you will be ready to apply configuration profiles to those devices.

1. Browse to Teams admin center (https://admin.teams.microsoft.com) as the Teams device administrator (youruser@<YourTenant>.onmicrosoft.com).
2. In **Teams admin center**, on the left navigation pane, select **Phones** under **Teams devices**.
3. On the **Phones** page, select **Configuration profiles** tab, and then select **+ Add**.
4. Enter the following information for the new configuration profile:
    - Configuration profile Name: **New York Teams Desk Phones**
    - Description: **Configuration profile for Teams Desk Phones in New York HQ**
5. Under **General** section, configure following settings:
    - Device lock: **On**
    - Timeout: **30 seconds**
    - PIN: **123456**
    - Language: English **(United States)**
    - Timezone: **(UTC-5:00) Eastern Time (US and Canada)**
    - Date format: **MM/DD/YYYY**
    - Time format: **12 Hours (AM/PM)**
6. Under **Device settings** configure following settings:
    - Display screen saver: **On, Timeout 1 minute**

- Display high contrast: **On**
- Office hours: **08:00-17:00**
- Power Saving: **On**

7. Under **Network settings**, configure following settings:
   - DHCP enabled: **On**
   - Logging enabled: **Off**
   - Device's default admin password: **Pass@word1**
8. Once you complete with the configuration profile settings, select **Save**.
9. Sign out and close all browser windows.

In this task, you have successfully created a configuration profile that can be applied to Microsoft Teams devices.

Task 2 - Configure a resource account for Teams Room

Your organization has ordered devices for Microsoft Teams room. In the meantime, you need to ensure that all prerequisites for the equipment installation are being completed. One of the prerequisites for Microsoft Teams Room deployment is adding a device account and assigning Office 365 license for that account.

1. Browse to Microsoft 365 admin center (https://admin.microsoft.com/).
2. Create a Microsoft 365 resource account for Teams Rooms.
   i. In left navigation of the Microsoft 365 admin center, select **Show all** > **Resources** > **Rooms & equipment**. If you don't find **Resources**, search for **Rooms & equipment** from the top search bar and select.
   ii. On the Rooms & equipment screen, select the **+ Add resource** option to add a new resource account.
   iii. On the **Add resource** page, follow the wizard with the following information.
      - Resource type: **Room**.
      - Name: **NY-TeamsRoom1**

- Email: Enter **NY-TeamsRoom1** inside the Email text box and verify your tenant id in the domains

iv. Select **Save**.

v. Select **Edit booking options**, keep the default settings with the following checked.

- Allow repeating meetings
- Automatically decline meetings outside of the limits
- auto-accept meeting requests

3. Get Microsoft Teams Rooms Pro trial licenses

   i. In the **Microsoft 365 admin center** from the left navigation pane, under **Billing** select **Purchase services**.

   ii. In the **Search** box on the right, type **Meeting Room** and then hit Enter.

   iii. In the results page, locate the **Collaboration and communication** section, and under **Microsoft Teams Rooms Pro** tile, select **Details** and then select **Start free trial**.

   iv. In the **Check out** page, select **Try now**, and in the **order receipt** page, select **Continue**.

4. Assign the license to the Teams Rooms account.

   i. In the **Microsoft 365 admin center** from the left navigation pane, select **Users**, and then choose **Active Users**.

   ii. Select the NY-TeamsRoom1@<YourTenant>.onmicrosoft.com account, and then select the **Licenses and Apps** tab.

   iii. In the NY-TeamsRoom1@<YourTenant>.onmicrosoft.com page, under the **Licenses and Apps** tab, select **Microsoft Teams Rooms Pro** and then select **Save changes**.

5. Sign out and close all open windows.

You have successfully created, configured, and licensed a Microsoft Teams Room service account, which is a prerequisite for deploying a Microsoft Teams Room system.

Exercise 3: Set up a Calling Plan (Optional)

In this exercise, you will set up one of your users with a Calling Plan Trial. You will need to start the trial, order a phone number from Microsoft as your provider and enable your user to use this phone number when making outgoing calls.

Note: The availability of Calling Plans varies based on different countries and regions. Please go to the link below to check the availability of your location. The following instruction is based on the location of the United States.

https://docs.microsoft.com/en-us/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans/country-and-region-availability-for-audio-conferencing-and-calling-plans

Task 1 - Add a new emergency address

In this task, you will add a new emergency address "One Microsoft Way, Redmond, WA 98052, USA" for users in the United States. It is used to route emergency calls to the appropriate dispatch authorities and to assist in locating the emergency caller.

1. Browse to the **Teams admin center** at **https://admin.teams.microsoft.com/** (youruser@<YourTenant>.onmicrosoft.com).
2. On the left navigation pane select **Locations** > **Emergency addresses**.
3. Select **+ Add** from the top pane to create a new emergency address.
4. On the **Emergency addresses\New emergency address** page, enter the following information:
    - Put in a name for your location: **Your organization Emergency Address**
    - Country or region: **United States**
    - Address: **1 Microsoft Way, Redmond, WA 98052**

      (You can enable **Input address manually**, and enter the address manually)
5. Acknowledge the emergency calling disclaimer. An information page opens, either **Print** or **Cancel** the page and continue to the next task.
6. Select **Save**.

7. Sign out and close the browser.

You have successfully created an emergency address that can be used for phone numbers.

Task 2 – Activate a trial Calling Plan

In this task, you will activate the Calling Plan Add-on Trial for your tenant so you can assign the calling plan to your users.

1. Sign in with the Credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft 365 admin center** at **https://admin.microsoft.com/**.
3. On the **Pick an account** page, (youruser@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Open the Navigation Menu in the upper left corner and select **Billing > purchase services**.
5. Select **Add-ons**.
6. Scroll down until you see **Microsoft Teams Domestic Calling Plan** (you may have to select **See more add-ons products**) and select **Details**.
7. Select **Start free trial**.
8. Select **Try now** to get 25 Calling Plans for a month.
9. Select **Continue** to continue past the order receipt.

You now have 25 Calling Plan licenses to assign to your users to test Domestic Calling Plan capabilities.

Task 3 – Assign a Calling Plan license to a user

In this task, you will assign the calling plan license to a user to allow them to make domestic calls via the public switched telephone network.

1. Sign in with the Credentials that have been provided to you.
2. You should still be in the **Microsoft 365 admin center** and signed (youruser@<YourTenant>.onmicrosoft.com).

3. Open the Navigation Menu in the upper left corner and select **Users**.
4. Select **Active users**.
5. Search for **Lynne Robbins** and open the additional settings by selecting her name.
6. Select **Licenses and apps**.
7. Under **Licenses** select **Microsoft Teams Domestic Calling Plan** by setting the checkmark in front of it.
8. Select **Save Changes** to assign the license and then sign out and close all open windows.

You have assigned the Calling Plan license to a user. With this license assigned your users can use the Calling Plan features and receive a phone number.

Task 4 – Order a phone number for your user

In this task, you will order a phone number for a user with an assigned Calling Plan license.

1. Sign in with the Credentials that have been provided to you.
2. In the **Microsoft Teams client** sign in (youruser@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
3. Navigate to the **Teams admin center** at **https://admin.teams.microsoft.com/**.
4. On the left navigation pane, select **Voice**, and then **Phone numbers** below.
5. Select **+ Add** in the right pane.
6. Type **Phone number order** as the **Order Name**.
7. Fill out the description as **Number for Lynne Robbins during the Calling Plan trial**.
8. In the dropdown menu of **Country or region**, select **United States**.
9. For **Number Type** select **User (Subscriber)**.

10. For the **Operator**, pick **Microsoft**.
11. For **Quantity** type **1**.
12. In the **Search for new numbers** section, you can use one of the following approaches to find new numbers:
    - Search by city name
        - Select **Search by city name**.
        - Search **Redmond** and select **Your organization Emergency Address**, which is the location you just created.
        - Select Area code **425**.
        - Select **Next**.
    - Search by area code
        - Select **Search by area code**.
        - Enter an area code in United States.
        - Select **Next**.

    Note: If you received the following message, please try other area codes or create another location by selecting **Add a location** which is next to the **Search by city name**. It will navigate to the **New emergency address** pane, enter the new name for the emergency address, then in the **Country or region** select **United States** and enter the new address manually in the **Address** field by enabling the slider **Input address manually** and select **Save**. It takes back to the **Get Phone numbers** page and continues the city search with the newly created emergency address to acquire the phone number.

    We can't find any phone numbers for the address you selected.
13. Once you reserved a phone number successfully, you can proceed by selecting **Place order**, then **Finish**.

Note: It might take some time for the phone numbers to show up. You can check your order from the **Order history** tab.

You just ordered a phone number for a User in Microsoft Teams. This is the same process you use to order numbers for all other Microsoft Teams services such as Call Queues.

Task 5 – Assign a phone number to your user

In this Task, you will assign an existing phone number to a user.

1. Sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed (youruser@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, select **Voice**, and then **Phone numbers** below.
4. Select the phone number you want to assign and select **edit** to open the options.
5. Under **Assigned to** search for **Lynne Robbins** and select **assign**.
6. Under **Emergency Location** select **Search by the location description**.
7. Type **Your organization** to search for the emergency location you created earlier.
8. Select **Apply** to assign the phone number to the user.

Exercise 4: Manage Teams Phone

Your organization organization is using the legacy PBX system. With the introduction of Microsoft Teams, Your organization will migrate their legacy telephony system to Microsoft Teams Phone. Teams admins are responsible for evaluating and testing Microsoft Teams voice functionalities.

Task 1 - Create a calling policy

As part of your pilot project for calling functionalities with Microsoft Teams, you have the requirement that all pilot users receive access to the voicemail functionalities. You create and assign a new calling policy and configure the settings. However, all other users should not receive voicemail functionalities during the testing period. Therefore, you will edit the default policy to ensure that voicemail is disabled for all other users.

1. Sign in with the Credentials that have been provided to you.

2. You should still be in the **Teams admin center** and sign in (youruser@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, select **Voice**, and then **Calling policies** below.
4. Select the **Global (Org-wide default)** policy to edit the default settings.
5. In **Calling policies\Global**, use the dropdown menu to the right of **Voicemail is available for routing inbound calls** and select **Not Enabled**. Then select **Save**.
6. Back on the **Calling policies** page, select **+ Add** on the top pane, to create a new policy.
7. Enter the following information:
    - Add new calling policy: **Voicemail enabled pilot users**
    - Description: **Calling policy that allows voicemail for selected pilot users**.
    - Voicemail is available for routing inbound calls: **Enabled**
8. Select **Save** to create the new policy.
9. Back on the **Calling policies** page, use the checkbox left to the **Voicemail enabled pilot users** policy and then select **Assign users** from the top pane.
10. In the right-side pane, type into the search field **Megan** then select **add**. Repeat the same steps for **Alex, Joni and Lynne**.
11. Select **Apply** to assign the policy to the selected users.

In this task, you have disabled voicemail for all users in the organizations, and then you have created a calling policy that will enable voicemail for several users.

Task 2 - Create a call queue

Your organization Ltd. has deployed Microsoft Teams voice functionalities throughout the organization. To deploy some automation for incoming support calls, the calling queue functionalities need to be tested before being rolled out. The following settings shall be configured for customers calling in:

1. A greeting message.

2. Music while people are waiting on hold.
3. Redirecting calls to call agents in mail-enabled distribution lists and security groups.

As Teams admin, you are responsible for creating the call queue and configuring different parameters, such as maximum queue size, timeout, and call handling options.

1. Sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in (youruser@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, select **Voice**, and then choose **Resource accounts,** to create a resource account.
4. On the **Resource accounts** page, select **+ Add** from the top pane.
5. On the right pane, enter the following information:
    - Display name: **Your organization Call Queue Resource Account**
    - Username: **pilot_callqueue1**
    - Resource Account Type: **Call queue**
6. Select **Save**.
7. Download the file **Alarm03.wav** from the following link and save to the Downloads folder.

    https://github.com/MicrosoftLearning/MS-700-Managing-Microsoft-Teams/blob/master/Instructions/Labs/media/Alarm03.wav
8. On the left navigation pane, select **Voice** and **Call queues**, to create a call queue.
9. Select **+ Add** from the top pane.
10. Enter the following information:
    - Call queue name: **Your organization Call Queue**
    - You haven't added any resource accounts yet: Select **Add**. On the right-side pane, search for **Your organization**, select **Add** from **Your organization Call Queue**, and then select **Add**.

- Language: **English (United States)**
- Greeting: select **Play an audio file**, and then select **Upload file**.
- In **Open** window, navigate to the Downloads folder, select **Alarm03.wav** and select **Open**.
- Music on hold: **Play default music**
- Call answering: Select **Choose users and groups** then select **Add groups** and on the right-side pane, search for **Sales**, select **Add** for **Sales** and then select **Add** at the bottom of the **Add call agents** pane.
- Routing method: **Round robin**
- Presence-based routing: **Off**
- Call agents can opt out of taking calls: **On**
- Call agent alert time: **30 seconds**
- Maximum calls in the queue: **50**
- When the maximum number of calls is reached: **Disconnect**
- Call time out handling maximum wait time: **5 minutes**
- When call times out: **Disconnect**

11. Select **Submit** to create the new call queue.

Creating the new call queue may take some time, but you have successfully created a new custom call queue based on a resource account in your tenant.

Note: Because this call queue shall have a custom greeting, you need to upload some wav files for demonstration purposes. In a real-world scenario, you would record and prepare a greeting audio file and upload the audio file as shown in this task.

Task 3 - Create an auto attendant

As Teams admin, you were tasked to create an auto attendant with a transcribed welcome message that will respond to customers outside of office hours. As some of your employees work in different time zones, the auto-attendant informs a caller that

the subscriber is currently on vacation and to call another person in the organization. Furthermore, the auto-attendant informs callers about business hours.

1. Sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and sign in (youruser@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, select **Voice**, and then choose **Resource accounts,** to create the resource account first.
4. On the **Resource accounts** page, select **+ Add** from the top pane.
5. On the right pane, enter the following information:
    - Display name: **Your organization Auto Attendant**
    - Username: **pilot_autoattendant1**
    - Resource Account Type: **Auto attendant**
6. Select **Save**.
7. On the left navigation pane, select **Voice** and then **Auto attendants** below.
8. Select **+ Add** from the top pane, to create a new auto-attendant.
9. Enter the following information:
    - Add a name for your auto attendant: **Your organization Auto attendant**
    - Operator: **Voice app**
    - Search by resource account: **Your organization Call Queue Resource Account**
    - Time zone: **(UTC-08:00) Pacific Time (US & Canada)**
    - Language: **English (United States)**
    - Enable voice inputs: **Off**
10. Select **Next**.
11. On the **Call flow** page, configure the following:

- First, play a greeting message: Select **Add a greeting message**
- Type in: **Welcome. The person you called is currently on vacation, your call will be redirected to an operator.**
- Then under Call routing options select **Redirect call**
- Redirect to: **Voice app**
- Search by resource account: **Your organization Call Queue Resource Account**

12. Select **Next**.
13. On the **Set business hours** page, configure the following:
    - Select **Clear all hours**
    - Configure working hours **Monday** to **Friday** from **08:00 AM** to **04:00 PM**
    - Leave **Saturday** and **Sunday** blank.
    - First, play a greeting message: **Add a greeting message**
    - Type in: **Thank you for your call, our business hours are Monday to Friday, 08:00 AM to 04:00 PM.**
    - Then route the call: **Disconnect**
14. Select **Next**.
15. On the **Holiday call settings** page, select **Next**.
16. On the **Dial scope** page, select **Next**.
17. On the **Resource accounts** page, select **Add**. In the right-side pane, type **Your organization auto attendant**, and then select **Add** twice.
18. Select **Submit** to finish the creation of the auto attendant.
19. Close all browser windows.

You have successfully created a resource account for the auto attendant and then created an auto attendant configuration.

Exercise 5: Explore reports for call quality in Microsoft Teams

When users experience calling problems, an organization's Teams administrator must quickly diagnose and fix the problems. The Teams client, the network, and any number of configuration issues in the Microsoft Teams admin center can disrupt an organization's users from effectively sending and receiving calls and participating in Teams meetings.

In this exercise, you'll explore the monitoring and troubleshooting tools available in Teams admin center, including call analytics, and the call quality dashboard to investigate voice issues.

Note: As we have not made any calls in this environment, reports will be blank and incomplete.

Task 1 – Explore call analytics for users, calls, and meetings

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In the left-hand navigation pane, select **Users>Manage users**, and then select a user.
3. On the **User** page, select **Meetings & calls** tab.
4. Call analytics page displays all calls and meetings for the selected user,

By selecting a session in the list, you can view other information about a given session, including detailed media and networking statistics for call and meeting activities.

Task 2 – Explore Call Quality Dashboard (CQD)

CQD is designed to help Microsoft Teams administrators and network engineers monitor call and meeting quality at an organization-wide level. The near real-time data enables Teams admins to quickly resolve issues by drilling down to find where issues originated, and who was affected.

In this task you navigate to Call Quality Dashboard

1. Browse to Teams admin center (https://admin.teams.microsoft.com) (youruser@<YourTenant>.onmicrosoft.com).
2. In the left-hand navigation pane, select **Call Quality Dashboard** at the bottom.

3. A new browser tab with the url **https://cqd.teams.microsoft.com/** will open. You will be prompted to sign-in, when you access the CQD portal for the first time.

4. When you first sign into the CQD Portal, you'll see the summary reports with daily and monthly call quality trends. Call quality is classified as good, poor, or unclassified.

5. From the **Product Filter** dropdown menu, select **Microsoft Teams**.

6. Explore the data under different tabs, including Overall Call Quality, Server-Client, Client-Client, and Voice Quality SLA.

In this exercise you have learnt how to access and navigate call analytics and Call Quality Dashboard.

END OF LAB