Contents

1 MS-700: Managing Microsoft Teams

- **Download Latest Student Handbook and AllFiles Content**
- **Are you a MCT?** - Have a look at our GitHub User Guide for MCTs
- **Need to manually build the lab instructions?** - Instructions are available in the MicrosoftLearning/Docker-Build repository

1.1 What are we doing?

- To support this course, we will need to make frequent updates to the course content to keep it current with the Microsoft 365 services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Microsoft 365 platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Microsoft 365 changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

1.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Microsoft 365 services, and get the latest files for their delivery.

1.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

1.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.

- You can submit bugs, changes, improvement and ideas. Find a new Microsoft 365 feature before we have? Submit a new demo!

1.5 Notes

1.5.1 Classroom Materials

1.6 It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require them to access yet another UI as part of the course, contributing to a confusing experience for the student. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

1.7 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

2.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/MS-700-Managing-Microsoft-Teams/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

2.3 {% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MS-700-Managing-Microsoft-Teams/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.4 demo: title: 'Demo: Deploying an ARM Template' module: 'Module 1: Exploring Azure Resource Manager'

3 Demo: Deploying an ARM Template

3.1 Instructions

1. Quisque dictum convallis metus, vitae vestibulum turpis dapibus non.
    1. Suspendisse commodo tempor convallis.
    2. Nunc eget quam facilisis, imperdiet felis ut, blandit nibh.
    3. Phasellus pulvinar ornare sem, ut imperdiet justo volutpat et.
2. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.
3. Vestibulum hendrerit orci urna, non aliquet eros eleifend vitae.
4. Curabitur nibh dui, vestibulum cursus neque commodo, aliquet accumsan risus.

   ```
   Sed at malesuada orci, eu volutpat ex
   ```

5. In ac odio vulputate, faucibus lorem at, sagittis felis.
6. Fusce tincidunt sapien nec dolor congue facilisis lacinia quis urna.

Note: Ut feugiat est id ultrices gravida.

7. Phasellus urna lacus, luctus at suscipit vitae, maximus ac nisl.
    - Morbi in tortor finibus, tempus dolor a, cursus lorem.
    - Maecenas id risus pharetra, viverra elit quis, lacinia odio.
    - Etiam rutrum pretium enim.
8. Curabitur in pretium urna, nec ullamcorper diam.

3.2 lab: title: 'Lab 01: Manage roles and create teams' type: 'Answer Key' module: 'Module 1: Microsoft Teams in Microsoft 365'

4 Lab 01: Manage roles and create teams

5 Student lab answer key

5.1 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.**

5.2 Lab Scenario

In the labs, of this course, you will assume the role of **Joni Sherman**, a Teams Administrator for Contoso Ltd. and her pilot team that shall evaluate the capabilities of Microsoft Teams in a testing environment. You have implemented Microsoft 365 in a virtualized lab environment already and were commissioned to conduct a pilot project to test the implementation of Microsoft Teams against Contoso Ltd. business requirements.

You have just started the pilot project, and you've already got two virtual machines with preinstalled Teams Desktop clients and a tenant with different users:

- Joni Sherman (JoniS@<YourTenant>.OnMicrosoft.com) **Group coordinator / Teams admin**
- Alex Wilber (AlexW@<YourTenant>.OnMicrosoft.com) **Regular pilot user from Canada**
- Lynne Robbins (LynneR@<YourTenant>.OnMicrosoft.com) **Regular pilot user**
- Allan Deyoung (AllanD@<YourTenant>.OnMicrosoft.com) **Teams communication support engineer**
- Megan Bowen (MeganB@<YourTenant>.OnMicrosoft.com) **Regular employee**

5.3 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 it's menus
- Install the Teams PowerShell module and explore its cmdlets
- 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

5.4 Lab Setup

- **Estimated Time:** 60 minutes.

5.5 Instructions

5.5.1 Before you start

The lab in this course have been prepared for a Microsoft Teams deployment at Contoso Ltd. Corporation. Contoso 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. You will be provided with two virtual machines and a Microsoft 365 tenant to complete the lab steps.

5.5.1.1 1. Sign in to the lab virtual machines

The labs in this course will use two virtual machines:

- Client 1 VM : a stand-alone Windows 10 client virtual machine with Microsoft Teams pre-installed.
- Client 2 VM : a stand-alone Windows 10 client virtual machine with Microsoft Teams pre-installed.

Note: Lab virtual machine sign in instructions will be provided to you by your instructor.

Important: The exercises in the MS-700 labs are cloud-only deployments. A local administrator account has been created on the client VMs. You will log into the VMs as a local administrator instead of a domain account. Following your login, the desktop will indicate that you are logged in as either **CLIENT1\Admin** or **CLIENT2\admin**, depending on which machine you are on.

5.5.1.2 2. Review installed applications

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

- Microsoft Teams

5.5.1.3 3. Review Microsoft 365 tenant

Beside two VMs, you will also be provided with a Microsoft 365 tenant with following highlights:

- Office 365 E5 with Enterprise Mobility + Security E5.
- 15 licenses in total with 5 available of 15(10 used).
- One Global Administrator (MOD Administrator) and 9 standard users have been pre-created.

  Note: Microsoft 365 sign in instructions will be provided to you by your instructor.
- The username of the Global Administrator (MOD Administrator) is **admin@<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.

  IMPORTANT: This is critical because throughout this lab, you will be asked to enter the **<YourTenant>.onmicrosoft.com** domain name when signing into apps with a given username (for example, JoniS@<YourTenant>.onmicrosoft.com). When doing so, you must enter the unique tenant suffix ID that is assigned to your tenant ID in place of the **<YourTenant>**.

  For example, if your Tenant Email is **admin@contosolab.onmicrosoft.com**, the unique tenant suffix ID (<YourTenant>) is **contosolab**. When signing in as Joni when entering this domain, you would replace <YourTenant> with contosolab (for example, JoniS@contosolab.onmicrosoft.com).

  RECOMMENDATION: You should write down your unique tenant suffix, mentioned as <YourTenant> in this lab and provided by your training provider. After a while, you will have this name or number memorized as you move through the labs in this course.
- **Use the new Microsoft 365 admin center**

  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 exercises for this course are based on the new Microsoft 365 admin center UI and not the classic UI.

5.5.2 Exercise 1: Prepare team roles and licenses

In the first exercise you will assign required administrative roles to users, check license assignments for the Teams license and then explore the Microsoft Teams admin center. To perform these tasks, you will use default tenant global admin and the Joni Sherman's account (JoniS@<*YourTenant*>.onmicrosoft.com).

5.5.2.1 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 context of Joni Sherman's account.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open **Microsoft Edge** and navigate to the **Office 365 Portal** at **https://portal.office.com/**.
3. When the Sign in window is displayed, sign in as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) using the credentials provided to you.
4. On the **Stay signed in?** dialog box, select the **Don't show this again** checkbox and then select **No**.
5. Close the password save dialog from the bottom with **Never**, not to save the default global admins credentials in your browser.
6. If a welcome screen is displayed, close it. If the Office 365 apps notification appear, also close it.
7. Select the app launcher icon in the upper-left and choose **Admin**.
8. If a welcome window is displayed, select **Get started** and close it.
9. Select the navigation menu in the upper-left and select **Users** and **Active users** from below it.
10. In the Active users list, search and select **Joni Sherman**, to open the right-side settings pane.
11. In the settings below the Account tab, scroll to **Roles** and select **Manage roles** below.
12. When the **Manage roles** pane opens, select **Admin center access** and scroll down to select **Show all by category** to reveal all avaliable roles. Select the **Teams Administrator** and **Teams Device Administrator** roles.
13. Select **Save changes** to apply the role. When the **Admin roles updated** message is displayed on the upper part of the pane, close the window of Joni Sherman's account with the **X** in the upper right to go back to the **Active users** list.
14. Search for **Allan Deyoung** in the list of users, and select his name to open another settings pane.
15. In the settings below the Account tab, scroll to **Roles** and select **Manage roles** below.
16. When the **Manage roles** pane opens, select **Admin center access** and scroll down to the end and select **Show all by category**. Then scroll further down and select the **Teams communication support engineer** role.
17. Select **Save changes** to apply the role. When the **Admin roles updated** message is displayed, close Allan's profile pane and leave the client open at the Microsoft 365 admin center.

You have now successfully assigned the Teams Administrator role to Joni Sherman and the Teams communications support engineer to Allan Deyoung. Proceed to the next task.

5.5.2.2 Task 2 – Check license assignment of your users

In this task, you will check the license assignment of all users participating in the pilot. You will continue where you left off in the last task, signed in as the MOD Administrator on Client 1 VM, with an open browser window in the Microsoft 365 admin center. At the end of the task you will confirm that all pilot users are licensed correctly and change Alex's location to Canada as preparation for a later task.

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

2. You should still be signed in to the **Microsoft 365 admin center** (https://admin.microsoft.com/) as the **MOD Administrator**.
3. If you are not already on the **Active users** page, open the left side pane, select **Users** and **Active users** below.
4. In the Active users list, select **Alex Wilber** to open the right-side settings pane.
5. From the now visible tabs, select **Licenses and Apps**.
6. Check if the dropdown menu below **Select location** is set to **United States**. Change it to **Canada**. Then select **Save changes** at the end of the window and continue with the next step.

   Note: If you possibly receive an error message, deselect all licenses and select them again to process the assignment correctly and to make the location change work.
7. Below **Licenses**, verify that **Enterprise Mobility + Security E5** and **Office 365 E5** are both selected with a checkmark.
8. Select the dropdown arrow right beside **Apps** to open the view for the single licenses.
9. Scroll down the list of all apps to **Microsoft Teams** with **Office 365 E5** listed below it and validate this entry has a checkmark left of it. This indicates that the user has a valid Teams license from the Office 365 E5 subscription package assigned.
10. Close the window with the **X**, below the circle with the MA, which stands for the currently signed in user **MOD Administrator**.
11. Repeat the steps 3 to 9 for the users **Joni Sherman**, **Lynne Robbins**, **Allan Deyoung** and **Megan Bowen** to check their assigned licenses, but skip step 6 and do not change their location.
12. After checking the licenses of all users, leave the browser open with the Microsoft 365 admin center.

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.

5.5.2.3 Task 3 - Explore Teams Admin center

You need to test access and review the available settings for administering Teams in the Teams admin center. As an administrator for Teams, it's important to get to understand the different settings and policies available in the Microsoft Teams Admin Center. You will sign in with Joni Sherman's account for this task:You assigned the Teams Service Administrator role in the first task.

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

   Note: You should still be signed into Office 365 as **MOD Administrator**. You will sign out this user and sign in with Joni Sherman's account, to perform this task.
2. In the browser window, select the circle with **MA** in the upper right corner, open the side pane and select **Sign out**.
3. Close your browser window and re-open **Microsoft Edge** again and navigate to **https://admin.teams.microsoft.com** to open the Teams admin center.
4. When the **Pick an account** window is displayed, select **Use another account**. Sign in as (JoniS@<YourTenant>.onmicrosoft.com) using the credentials provided to you.
5. The Microsoft Teams admin center **Dashboard** is displayed. If a **Welcome to the Teams admin** center message is displayed, select **Skip tour**.
6. Select the navigation button in the upper-left to maximize the left-side pane and hover over the first symbol below, which is named **Teams**. Select **Manage Teams**.
7. On the **Manage teams** page, the teams existing in your organization are displayed. Note that there is a single org-wide team named **Contoso** that is automatically created for organizations with less than 5000 users that are new to Teams.
8. Select **Teams policies** in the left navigation. In the middle of the screen, the Teams policies are displayed. Note that there is a single policy named **Global (Org-wide default)**. Select the **Global (Org-wide**

default) policy to open a right-side settings pane and review the configured default global settings. Do not make any changes and then select **Cancel**.

9. Repeat the last steps for the other menus in the left navigation as you wish and explore the different default policies and settings. Do not make any changes and just explore the UI to understand the structure and options the Teams admin center provides.
10. When you are finished reviewing all settings from the Teams admin center, leave the client open as it is.

You have successfully explored several available menus from the Teams admin center, for managing teams and configuring policies in your tenant. You have finished the first exercise, and you can continue with the next one.

5.5.3 Exercise 2: Explore PowerShell cmdlets for Teams

In this exercise you will install the Teams PowerShell module, 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 also in the PowerShell. You can create scripts for automation and even access several settings not available in the GUI.

5.5.3.1 Task 1 - Install Teams PowerShell module

Before you can connect to Teams from your tenant and perform any actions, you need to install the Teams PowerShell module. You can install the Teams PowerShell module from the available repositories preconfigured in your Windows 10 operating system and do not need to download any executables via the browser.

Note: The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks when done on servers.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right select the **Start** button and then select **Windows PowerShell (Admin)**.
3. Confirm the **User Account Control** window with **Yes**.
4. In the PowerShell window, enter the following cmdlet and press **Enter**, to change the execution policy:

   ```
   Set-ExecutionPolicy Unrestricted
   ```

5. Enter **Y** and press **Enter** to confirm the security dialog for **Executing Policy Change**.
6. To install the Microsoft Teams module from the PsGallery repository, in the PowerShell window, enter the following cmdlet and press **Enter:**

   ```
   Install-Module -Name MicrosoftTeams
   ```

7. When you are prompted to install and import the NuGet provider, confirm by entering **Y** and pressing **Enter**.
8. When you are prompted to install from the Untrusted repository, also confirm by entering **Y** and pressing **Enter**.
9. Close the elevated PowerShell window and continue to the next task.

You have now successfully installed the latest available Microsoft Teams PowerShell module from the PSGallery repository. Continue with the next task.

5.5.3.2 Task 2 - Explore Teams PowerShell cmdlets

In this task, you will connect with the Teams PowerShell module to your tenant and explore the available cmdlets and functions to manage your tenant.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right select the **Start** button and then select **Windows PowerShell**.
3. To connect to Microsoft Teams in your tenant, enter the following cmdlet in the PowerShell window and press **Enter**:

   ```
   Connect-MicrosoftTeams
   ```

4. A **Sign in** dialog box will open. Sign in as (JoniS@<YourTenant>.onmicrosoft.com) using the Credentials provided to you.
5. When the sign in was successful, several information about the signed in user and the tenant are displayed. To confirm the MicrosoftTeams module is loaded correctly, enter the following cmdlet and press **Enter** to view all available PowerShell modules:

   ```
   Get-Module
   ```

   Note: To the left of the **Name** column, the version of the PowerShell module is displayed.
6. To get an overview of the available Teams PowerShell cmdlets from the MicrosoftTeams module for managing Teams, enter the following cmdlet and then press **Enter**:

   ```
   Get-Command -Module MicrosoftTeams
   ```
7. The Get-Help cmdlet is used explore the available cmdlets. For example, to get more information about how to create a team with PowerShell, enter the following cmdlet and press **Enter**:

   ```
   Get-Help New-Team
   ```
8. If you receive a message to update the help libraries, type **Y** for yes.
9. When you are finished with exploring the Microsoft Teams PowerShell cmdlets, close the PowerShell window.

You have successfully used the Microsoft Teams PowerShell module to connect to Teams in your tenant and explored some available cmdlets.

5.5.4 Exercise 3: Create groups and teams

In this exercise, you will create some resources required in later tasks. These include creating a Microsoft 365 Group from the Microsoft 365 admin center and creating a team in the Desktop client and then the web client.

5.5.4.1 Task 1 - Create a Microsoft 365 Group

In real world scenarios, the Microsoft 365 Groups would already exist and your task as Teams Administrator would only be to enable their Teams functionality, but for this lab you need to create them manually.

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

1. Connect to the **Client 1 VM** 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/** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. In the Microsoft 365 admin center, select the navigation menu in the upper-left, select **Groups** > **Active Groups**.
4. Select **Add a group** in the **Active groups** window to open the **Add a group** page.
5. Select the group type **Microsoft 365 (recommended)** and select **Next**.
6. Enter the following information to the text fields:
   - Name: **IT-Department**
   - Description: **All staff of the IT-Department**
7. Select **Next**.
8. In the Owners field type in the Name of **Joni Sherman**, select her from the **Users** list, and then select **Next**.
9. As the group email address type in **IT-Department**@<YourTenant>.onmicrosoft.com, set the privacy to **Private – Only members can see group content**, clear the **Create a team for this group** checkbox, and then select **Next**.
10. On the **Review** page, verify the settings and then select **Create group**.
11. When the **New group created** information appears, select **Close**.

12. Wait a moment and select **Refresh** until the group is visible. You will see there is no Teams icon in the **Teams status** column.
13. Select the **IT-Department** group to open the settings pane.
14. On the **Members** tab, select **View all and manage members**.
15. In the new window, select **+ Add members** from the top and select the checkbox before the following users: **Alex Wilber**, **Allan Deyoung**, **Lynne Robbins**, and **Megan Bowen**.
16. Select **Save,** then **Close** two times and close the IT-Department pane with the **X**.
17. Close the browser window.

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

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

To test the self-service capabilities of Teams, in this task, Megan Bowen 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 to the **Client 2 VM** with the credentials that have been provided to you.
2. Select the **Teams** icon on the taskbar to start the Teams Desktop client.
3. When prompted to **Enter your work, school or Microsoft account**. Sign in as (MeganB@<YourTenant>.onmicrosc using the O365 Credentials provided to you.
4. The Microsoft Teams Desktop client will start. If a **Bring your team together** window appears, or **Get the Teams mobile app**, or another message, close them with the **X** or **Try it now**.
5. If you are not already in the **Teams** overview, in the left-hand navigation pane, select **Teams.** Then, select **Join or create a team** from the lower end of the Teams list.
6. Select **Create team** in the middle of the window.
7. In the **Create your team** window, select **From scratch**, then select **Public**. Enter the team name **Teams Rollout** and select **Create**.
8. On the **Add members to Teams Rollout** window, enter the names of the desired team members and select their names to add them to the textbox: **Alex Wilber**, **Allan Deyoung**, **Joni Sherman**, and **Lynne Robbins**.
9. Select **Add** to add them to the team.
10. Wait for all four users to be listed on the **Add members to Teams Rollout** window as Members, and then change the status of Joni Sherman from **Member** to **Owner** with the dropdown menu.
11. Select **Close**.

You have successfully created a new team with the Teams Desktop client, added the project team members, and you have made Joni Sherman a second owner of the team. Close the Teams client and continue with the next task.

5.5.4.3 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 Megan Bowen as a member.

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft Teams web client** at **https://teams.microsoft.com**.
3. When the Sign in window is displayed, sign in as (LynneR@<YourTenant>.onmicrosoft.com) using the O365 credentials provided to you.
4. On the **Stay signed in?** dialog box, select the **Don't show this again** checkbox and then select **No**.
5. Close the password save dialog from the bottom with **Never**, not to save the default global admins credentials in your browser.

6. A landing page with a **Download the Teams desktop app and stay better connected** message is displayed. Select **Use the web app instead** below this message.
7. Another welcome message is displayed. Close all messages with **Try it now** or the **X**.
8. Select **Teams** from the left-side pane if you are not already in the **Teams** overview.
9. Select **Join or create a team** from the lower end of the Teams list.
10. Select **Create team** from the middle of the window.
11. In the **Create your team** window, select **From scratch**, then select **Private**. Enter the team name **Sales** and select **Create**.
12. In the **Add members to Sales** dialog, enter **Megan Bowen** to add her as a team member.
13. Select **Add** to add her to the team.
14. After adding the members to the Sales team, verify that Megan Bowen has been added correctly as a **Member**.
15. Select **Close**.
16. The newly created team is displayed in the list of your teams.
17. Close the Microsoft Edge window.

You have successfully created a new team with the Teams web client. This is the end of lab 1. You can close all browser windows and proceed to the next lab.

5.6 END OF LAB

5.7 lab: title: 'Lab 01: Manage roles and create teams' module: 'Module 1: Microsoft Teams in Microsoft 365'

6 Lab 01: Manage roles and create teams

7 Student lab manual

7.1 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.**

7.2 Lab Scenario

In the labs of this course you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. and her pilot team that shall evaluate the capabilities of Microsoft Teams in a testing environment. You have implemented Microsoft 365 in a virtualized lab environment already and were commissioned to conduct a pilot project to test the implementation of Microsoft Teams against Contoso Ltd. business requirements.

You have just started the pilot project, and you've already got two virtual machines with preinstalled Teams Desktop clients and a tenant with different users:

- Joni Sherman (JoniS@<*YourTenant*>.OnMicrosoft.com) **Group coordinator / Teams admin**
- Alex Wilber (AlexW@<*YourTenant*>.OnMicrosoft.com) **Regular pilot user from Canada**
- Lynne Robbins (LynneR@<*YourTenant*>.OnMicrosoft.com) **Regular pilot user**
- Allan Deyoung (AllanD@<*YourTenant*>.OnMicrosoft.com) **Teams communication support engineer**
- Megan Bowen (MeganB@<*YourTenant*>.OnMicrosoft.com) **Regular employee**

7.3 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
- Install the Teams PowerShell module and explore its cmdlets
- 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

7.4 Lab Setup

- **Estimated Time:** 60 minutes.

7.5 Instructions

7.5.1 Before you start

The lab in this course have been prepared for a Microsoft Teams deployment at Contoso Ltd. Corporation. Contoso 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. You will be provided with two virtual machines and a Microsoft 365 tenant to complete the lab steps.

7.5.1.1 1. Sign in to the lab virtual machines

The labs in this course will use two virtual machines:

- Client 1 VM : a stand-alone Windows 10 client virtual machine with Microsoft Teams pre-installed.
- Client 2 VM : a stand-alone Windows 10 client virtual machine with Microsoft Teams pre-installed.

Note: Lab virtual machine sign in instructions will be provided to you by your instructor.

Important: The exercises in the MS-700 labs are cloud-only deployments. A local administrator account has been created on the client VMs. You will log into the VMs as a local administrator instead of a domain account. Following your login, the desktop will indicate that you are logged in as either **CLIENT1\Admin** or **CLIENT2\admin**, depending on which machine you are on.

7.5.1.2 2. Review installed applications

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

- Microsoft Teams

7.5.1.3 3. Review Microsoft 365 tenant

Beside two VMs, you will also be provided with a Microsoft 365 tenant with following highlights:

- Office 365 E5 with Enterprise Mobility + Security E5.
- 15 licenses in total with 5 available of 15(10 used).
- One Global Administrator (MOD Administrator) and 9 standard users have been pre-created.

  Note: Microsoft 365 sign in instructions will be provided to you by your instructor.
- The username of the Global Administrator (MOD Administrator) is (admin<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.

IMPORTANT: This is critical because throughout this lab, you will be asked to enter the **<YourTenant>.onmicrosoft.com** domain name when signing into apps with a given username (for example, JoniS@<YourTenant>.onmicrosoft.com). When doing so, you must enter the unique tenant suffix ID that is assigned to your tenant ID in place of the **<YourTenant>**.

For example, if your Tenant Email is **admin@contosolab.onmicrosoft.com**, the unique tenant suffix ID (<YourTenant>) is **contosolab**. When signing in as Joni when entering this domain, you would replace <YourTenant> with contosolab (for example, JoniS@contosolab.onmicrosoft.com).

RECOMMENDATION: You should write down your unique tenant suffix, mentioned as <YourTenant> in this lab and provided by your training provider. After a while, you will have this name or number memorized as you move through the labs in this course.

- **Use the new Microsoft 365 admin center**

  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 exercises for this course are based on the new Microsoft 365 admin center UI and not the classic UI.

7.5.2 Exercise 1: Prepare team roles and licenses

In the first exercise, you will assign required administrative roles to users, check license assignments for the Teams license, and then explore the Microsoft Teams admin center. To perform these tasks, you will use default tenant global admin and the Joni Sherman's account (JoniS@*<YourTenant>*.onmicrosoft.com).

7.5.2.1 Task 1 - Assign Teams Admin Roles to users

In this task, you will use the default global admin to login to the Microsoft 365 admin center and assign several teams admin roles to different users. This task is crucial for the following tasks and exercises because you will perform most of the tasks in context of Joni Sherman's account.

1. Sign in to the **Microsoft 365 admin center** (**https://admin.microsoft.com**) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Assign the role of the **Teams Administrator** to **Joni Sherman**.
3. Assign the role of the **Teams communication support engineer** to **Allan Deyoung**.
4. Leave the client open at the **Microsoft 365 admin center**.

You have now successfully assigned the Teams admin role to Joni Sherman and the Teams communications support engineer to Allan Deyoung. Proceed to the next task.

7.5.2.2 Task 2 - Check license assignment of your users

In this task, you will check the license assignment of all users participating in the pilot. You will continue where you left off in the last task, signed in as the MOD Administrator on Client 1 VM, with an open browser window in the Microsoft 365 admin center. At the end of the task, you will confirm that all pilot users are licensed correctly and change Alex's location to Canada as preparation for a later task.

1. Navigate to the **Microsoft 365 admin center** (**https://admin.microsoft.com**) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Change the **Usage Location** of **Alex Wilber** to **Canada**.
3. Check, that all pilot users have the **Enterprise Mobility + Security E5** and **Office 365 E5** licenses assigned.
4. Close the **Microsoft 365 admin center**.

You have successfully validated, that all users participating in the pilot own Teams licenses and they 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.

7.5.2.3 Task 3 - Explore Teams Admin center

You need to access and review the available settings for administering Teams in the Teams admin center. As an administrator for teams, it's important to get to understand the different settings and policies available in the Microsoft Teams Admin Center. You will login with Joni Sherman's account for this task, that you assigned the Teams Administrator role in the first task.

1. Sign in to the **Teams admin center** **https://admin.teams.microsoft.com** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Navigate to the Teams admin page.
3. Navigate through the policies and settings menus.
4. Leave the **Teams admin center** opened.

You have successfully explored several available menus from the Teams admin center in managing teams and configuring policies in your tenant. You have finished the first exercise and you can continue to the next one.

7.5.3 Exercise 2: Explore PowerShell cmdlets for Teams

In this exercise you will install the Teams PowerShell module, required to manage teams, policy packages, telephony, and all other settings for Teams in your tenant. You can perform most of the tasks possible from the Teams admin center also in the PowerShell. You can script for automation and even access several settings not available in the GUI.

7.5.3.1 Task 1 - Install Teams PowerShell module

Before you can connect to Teams from your tenant and perform any actions, you need to install the Teams PowerShell module. You can install the Teams PowerShell module from the available repositories preconfigured in your Windows 10 operating system. You don't need to download any executables via the browser.

1. Open an elevated **Windows PowerShell (Admin)** window.
2. Change the current execution policy with cmdlet:

   ```
   Set-ExecutionPolicy Unrestricted
   ```

3. Install the mainstream Teams PowerShell module:

   ```
   Install-Module -Name MicrosoftTeams
   ```

4. Close the elevated PowerShell window.

You have now successfully installed the latest available Microsoft Teams PowerShell module from the PSGallery repository. Continue with the next task.

7.5.3.2 Task 2 - Explore Teams PowerShell cmdlets

In this task, you will connect with the Teams PowerShell module to your tenant and explore the available cmdlets and functions to manage your tenant.

1. Open a regular **Windows PowerShell** window.
2. Connect to Teams in your tenant using cmdlet:

   ```
   Connect-MicrosoftTeams
   ```

3. Check the installed modules using cmdlet:

   ```
   Get-Module
   ```

4. Investigate the available cmdlets:

   ```
   Get-Command -Module MicrosoftTeams
   ```

5. Use the help cmdlet for more information about the available cmdlets:

   ```
   Get-Help <cmdlet>
   ```

6. Close the PowerShell window.

When you are finished with exploring the Microsoft Teams PowerShell cmdlets, close the PowerShell window and continue to the next task.

7.5.4 Exercise 3: Create groups and teams

In this exercise, you will create some resources required in later tasks. These include creating a Microsoft 365 Group from the Microsoft 365 admin center and creating a team in the Desktop client and then the web client.

7.5.4.1 Task 1 - Create a Microsoft 365 Group

In real world scenarios, the Microsoft 365 Groups would already exist and your task as Teams Administrator would only be to enable their Teams functionality, but for this lab you need to create them manually.

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

1. Sign in to the **Microsoft 365 admin center** (**https://admin.microsoft.com**) as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Create and configure a new Microsoft 365 group with the following settings:
   - Name: **IT-Department**
   - Description: **All staff of the IT-Department**
   - Owners: **Joni Sherman**
   - Group email address: **IT-Department**@<YourTenant>.onmicrosoft.com
   - Privacy: **Private – Only members can see group content**
   - Create a team for this group: **Clear the checkbox**
   - Members: **Alex Wilber, Allan Deyoung, Lynne Robbins** and **Megan Bowen**
3. Close the **Microsoft 365 admin center**.

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

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

To test the self-service capabilities of Teams, in this task, Megan Bowen 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 to the **Client 2 VM** with the credentials that have been provided to you.
2. Connect to a client and sign in to the Teams Desktop client using **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft
3. Create a new team with the following settings:
   - Type: **Build a team from scratch**
   - Privacy: **Public**
   - Name: **Teams Rollout**
   - Owners: **Joni Sherman** and **Megan Bowen**
   - Members: **Alex Wilber**, **Allan Deyoung** and **Lynne Robbins**
4. Close the Teams Desktop client.

You have successfully created a new team with the Teams Desktop client, added the project team members and you have made Joni Sherman a second owner of the team. Close the Teams client and continue with the next task.

7.5.4.3 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 Megan Bowen as a member.

1. Sign in to the Teams web client (**https://teams.microsoft.com**) using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
2. Create a new team with the following settings:

- Type: **Build a team from scratch**
- Privacy: **Private**
- Name: **Sales**
- Owners: **Lynne Robbins**
- Members: **Megan Bowen**

3. Close the Teams web client.

You have successfully created a new team with the Teams web client. This is the end of lab 1. You can close all browser windows and proceed to the next lab.

7.6 END OF LAB

7.7 lab: title: 'Lab 02: Configure security and compliance for teams and content' type: 'Answer Key' module: 'Module 2: Implement Microsoft Teams Governance, Security and Compliance'

8 Lab 02: Configure security and compliance for teams and content

9 Student lab answer key

9.1 Lab Scenario

In the labs of this course, you will assume the role of the System Administrator for Contoso Ltd. Your organization is planning to deploy Microsoft Teams. Before starting the deployment, IT department is gathering business requirements about Teams governance as well as data security and compliance, including how the data shared in Teams be regulated according to the organization's compliance requirements. After you complete the planning process, you will configure Microsoft 365 Groups governance, protect Teams from threats, and configure Teams to meet your organization compliance requirements.

9.2 Objectives

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

- Activate, create and assign sensitivity labels
- Configure expiration policies
- Restrict creation of new teams to members of a security group
- Create naming policies
- Reset all Azure AD settings to defaults
- Activating Safe Attachments for SharePoint, OneDrive and Teams
- Create, configure and test retention policies
- Create and test a DLP policy to protect GDPR content

9.3 Lab Setup

- **Estimated Time:** 90 minutes.

9.4 Instructions

9.4.1 Exercise 1: Implement governance and lifecycle management for Microsoft Teams

Your organization has started the planning process for Microsoft 365 services adoption. You are assigned as 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, configuring and assigning sensitivity labels, creating Microsoft 365 groups expiration policies, configuring Microsoft 365 Group creation policy permissions, configuring and test Microsoft 365 Groups naming policies.

9.4.1.1 Task 1 – Activate sensitivity labels for Teams

You need to evaluate governance for Microsoft 365 Groups before deploying them in your organizations. In this task, you will activate the sensitivity labels for Teams in Azure AD, for being able to assign labels in a following task.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right select the **Start** button and then select **Windows PowerShell (Admin)**.
3. Confirm the User Account Control window with **Yes**.
4. Maximize the PowerShell window and enter the following cmdlet to install the **Azure AD Preview** module:

   ```
   Install-Module AzureADPreview
   ```

5. When you are prompted to install from the untrusted repository, confirm by entering **Y** and pressing Enter.
6. Type in the following cmdlet to connect to Azure AD in your tenant:

   ```
   Connect-AzureAD
   ```

7. A **Sign in** dialog box will open. Sign in as admin@<YourTenant>.onmicrosoft.com using the credentials provided to you.
8. To enable Microsoft 365 Groups and Teams for Sensitivity labels, you first need to load the Azure AD unified group template, by using the following cmdlet:

   ```
   $Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq "Group.Unified"}
   ```

9. Check if an Azure AD setting is already existing and load it, if yes. If not, create a blank Azure AD setting object. Run the following cmdlet to populate the "$Setting" variable:

   ```
   if(!($Setting = Get-AzureADDirectorySetting | Where {$_.TemplateId -eq $Template.Id})) {$Setting =
   ```

10. Enable the Microsoft Identity Protection (MIP) support in your configuration:

    ```
    $Setting["EnableMIPLabels"] = "True"
    ```

11. To verify the new configuration, run the following cmdlet:

    ```
    $Setting.Values
    ```

12. Save the changes and apply the setting:

    ```
    New-AzureADDirectorySetting -DirectorySetting $Setting
    ```

    Note: Since this is a new tenant, there's no directory settings object in the tenant yet. You need to use `New-AzureADDirectorySetting` to create a directory settings object at the first time.

    If there's an existing directory settings object, you will need to run the following cmdlet to update the directory setting in Azure Active Directory:

    ```
    Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
    ```

13. Close the PowerShell window.

You have successfully changed your tenants Azure AD settings and activated sensitivity labels for Microsoft 365 Groups and Microsoft Teams.

9.4.1.2 Task 2 - Create sensitivity labels for Teams

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

1. You are still connected to the **Client 1 VM**.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft 365 compliance center** at **https://compliance.microsoft.com/**.

3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. In the **Microsoft 365 compliance center**, on the left navigation pane, scroll down and select **…Show all** and select **Information protection** from the expanded left side navigation pane.
5. On the top part of the page, you can see a warning message in a yellow box that states: 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 on here, but note that additional configuration is required for Multi-Geo environments. Select **Turn on now** to activate content processing in Office online files.
6. Select **+ Create a label** to create a new sensitivity label.
7. On the **Name and create a tooltip for your label** page, enter the following information:
   - **Name**: General
   - **Display name**: General
   - **Description for users**: General information without protection
   - **Description for admins**: General information without encryption, marking or sharing restriction settings activated
8. Select **Next**.
9. Select **Files & emails** and **Groups & Sites** on the **Scope** page and select **Next**.
10. Do not make any changes on the **Choose protection settings for files and emails** page and select **Next**.
11. Do not make any changes on the **Auto-labeling for Office apps** page and select **Next**.
12. On the **Group & Sites** page, select both boxes **Privacy and external user access settings** and **External sharing and Conditional Access settings** and select **Next**.
13. On the **Define privacy and external user access settings** page select the following settings and then select **Next**:
    - **Privacy**: None-Team and group members can set the privacy settings themselves.
    - **External users access**: Select Let Microsoft 365 group owners add people outside the organization to the group.
14. On the **Define external sharing and device access settings** page select the following setting and then select **Next**.
    - **Unmanaged devices:** Allow full access from desktop apps, mobile apps, and the web.
15. Review your settings and select **Create label** to finish the new label creation.
16. When the **Your label was created** is displayed, select **Done**.
17. You should now see your newly created label "**General**" on the **Labels** dashboard. Select **+ Create a label** again, to create another sensitivity label.
18. On the **Name and create a tooltip for your label** page, 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
19. Select **Next**.
20. Select **Files & emails** and **Groups & Sites** on the **Define the scope for this label** page and select **Next.**
21. On the **Choose protection settings for files and emails** page, select both boxes **Encrypt files and emails** and **Mark the content of files** and select **Next**.

22. On the **Encryption** page, select **configure encryption settings** and perform the following configuration settings:
    - Assign permissions now or let users decide: **Assign permissions now**.
    - User access to content expires: **Never**.
    - Allow offline access: **Always**.
23. Select **Assign permissions** below **Assign permissions to specific users and groups**.
24. On the right-side pane, select **+ Add all users and groups in your organization**.
25. Select **Save** and **Next** to finish the Encryption settings.
26. On the **Content marking** page, select the slider and the checkbox **Add a watermark**.
27. Select **Customize text** to open the right-side pane.
28. Enter the following to the **Watermark text** box: **Internal use only**
29. Select **Save** and **Next**.
30. On the **Auto-labeling for Office apps** page, do not select the slider and select **Next**.
31. On the **Define protection settings for groups and sites** page, select both boxes **Privacy and external user access settings** and **External sharing and Conditional Access settings** and select **Next**.
32. On the **Define privacy and external user access settings** page, select the following settings and then select **Next**:
    - **Privacy**: None-Team and group members can set the privacy settings themselves.
    - **External users access**: Leave the box unchecked.
33. On the **external sharing** page, select the following setting and then select **Next**:
    - **Unmanaged devices:** Allow limited, web-only access.
34. Select **Next**.
35. Review your settings and select **Create label** to finish the new label creation.
36. When the **Your label was created** is displayed, select **Done**.
37. You should now see your newly created label "**Internal"** on the **Labels** dashboard. Select **+ Create a label** again, to create another sensitivity label.
38. On the **Name and create a tooltip for your label** page, enter the following information:
    - **Name**: Confidential
    - **Display name**: Confidential
    - **Description for users**: Confidential information with all protection
    - **Description for admins**: Confidential information with all restrictive encryption, marking and sharing settings activated
39. Select **Next**.
40. Select **Files & emails** and **Groups & Sites** on the **Define the scope for this label** page and select **Next**.
41. On the **Choose protection settings for files and emails** page, check both boxes **Encrypt files and emails** and **Mark the content of files** and select **Next**.
42. On the **Encryption** page select **configure encryption settings**:
    - Assign permissions now or let users decide: **Assign permissions now**
    - User access to content expires: **Never**
    - Allow offline access: **Never**
43. Select **Assign permissions** below **Assign permissions to specific users and groups**.

44. On the right-side pane, select **+ Add all users and groups in your organization**.
45. Select **Choose permissions** and select **Reviewer** from the dropdown menu, to restrict permissions.
46. Select **Save** twice.
47. Select **Next** to finish the Encryption settings.
48. On the **Content marking** page, select the slider and the checkbox **Add a watermark**.
49. Select **Customize text** to open the right-side pane.
50. Enter the following to the **Watermark text** box: Confidential.
51. Select **Save** and **Next**.
52. On the **Auto-labeling for Office apps** page, do not select the slider and select **Next**.
53. On the **Define protection settings for groups and sites** page, check both boxes **Privacy and external user access settings** and **External sharing and Conditional Access settings** and select **Next**.
54. On the **privacy & external users** page, select the following settings and then select **Next**:
    - **Privacy**: Private. Only team owners and members can access the group or team and, and only owners can add members.
    - **External users access**: Leave the box unchecked.
55. On the **external sharing** page select the following setting and then select **Next**:
    - **Unmanaged devices:** Allow limited, web-only access.
56. Select **Next**.
57. Review your settings and select **Create label** to finish the new label creation.
58. When the **Your label was created** is displayed, select **Done**.
59. Back on the **Information protection** page, select **Publish labels** from the top menu.
60. On the **Choose sensitivity labels to publish** page, select **Choose sensitivity labels to publish**.
61. Select the checkbox left from **Select all** and select **Add** to close the right-side pane.
62. Select **Next**.
63. On the **Publish to users and groups** page, do not make any changes to publish the label to all users.
64. Select **Next**.
65. On the **Policy settings** page, open the dropdown menu below **Apply this label by default to documents and email** and select **General** to use it as the default label for document and email.
66. Below **Apply this label by default to groups and sites**, also select the dropdown and select **General**.
67. Select **Next**.
68. On the **Name you policy** page, enter the following:
    - **Name**: All company sensitivity labels
    - **Enter a description for your sensitivity label policy**: Default sensitivity labels for all users in the company.
69. Select **Next**.
70. Review your settings and select **Submit** to publish the labels.
71. When **New policy created** is displayed, select **Done**.
72. Close the browser window.

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.

9.4.1.3 Task 3 - 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. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
3. On the Teams overview select the three dots (**...**) on the right side next to the Team "**Teams Rollout,"** then select **Edit team** from the dropdown list.
4. On the **Edit "Teams Rollout" team** window, select the dropdown menu below Sensitivity and select **Internal**.
5. Select **Done** to save the changes.

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

9.4.1.4 Task 4 - Create and assign an expiration policy

Based on the organization 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.

   Open **Microsoft Edge**, maximize the window and navigate to the **Azure Portal** at **https://portal.azure.com**. On the **Pick an account** page, select the global admin (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
2. If the **Welcome to Microsoft Azure** dialog box appears, select **Maybe later**. If an Azure Advisor recommendations window is displayed, close it with the **X**.
3. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
4. On the left navigation pane, select **Groups** and on the **Groups** page, on the left navigation pane, select **Expiration**.
5. In 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 (JoniS@<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**.
   - Select **Microsoft Azure** from the upper left in the Azure Portal and leave the Edge Browser window open.

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

9.4.1.5 Task 5 - Configure a group creation policy

You are an administrator for your Teams organization. You need to limit which users are able to 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right click the **Start** button and then select **Windows PowerShell**.
3. Connect to the Azure AD in your tenant with the following cmdlet:

   ```
   Connect-AzureAD
   ```

4. A Sign in dialog box will open. Sign in as admin@<YourTenant>.onmicrosoft.com using the O365 Credentials provided to you.
5. Create a new security group "GroupCreators" with the following cmdlet:

   ```
   New-AzureADGroup -DisplayName "GroupCreators" -SecurityEnabled:$true -MailEnabled:$false -MailNickl
   ```

6. Run following cmdlet to add **Lynne Robbins** to the new security group:

   ```
   Get-AzureADGroup -SearchString "GroupCreators" | Add-AzureADGroupMember -RefObjectId (Get-AzureADU
   ```

7. Fetch the current group settings for the Azure AD organization

   ```
   $Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where -Property DisplayN
   ```

8. Run following cmdlet to modify the group creation setting for your tenant with the "EnableGroupCreation" attribute:

   ```
   $Setting["EnableGroupCreation"] = "False"
   ```

9. Run following cmdlet to add the just created security group "GroupCreators" as permitted group to create groups, by their ObjectID:

   ```
   $Setting["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString "GroupCreators").objecti
   ```

10. Review the changes you have just configured with the following command:

    ```
    $Setting.Values
    ```

11. Then save the changes and apply the settings:

    ```
    Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
    ```

12. Close the PowerShell window.
13. To test the newly configured settings, connect to the **Client 2 VM** with the credentials that have been provided to you.
14. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
15. You won't see the option to **Create team**
16. Leave the client open and continue with the next task.

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.

9.4.1.6 Task 6 - 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 letters **Group** and end with the **Country** attribute of the Owners location. Furthermore, there is an internal regulation that forbids using following specific keywords in Teams names: CEO, Payroll and HR.

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

2. You are still signed in to the **Azure Portal**. If not, open **Microsoft Edge**, maximize the window and navigate to the **Azure Portal** at **https://portal.azure.com**.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
5. In the **Azure Active Directory**, on the left navigation pane, select **Groups**.
6. On the **Groups | All groups** page, on the left navigation pane, select **Naming policy**.
7. Select **Download** from the main window to download a blocked words sample file. Select **Save** and select **Open folder** on the lower end of the Edge browser window.
8. Right-click the file **BlockedWords.csv** and select **Edit** to open **Notepad**.
9. Type **CEO,Payroll,HR** replacing the empty quotes in the Notepad window, select **File** and **Save**. Afterwards, close the Notepad file.
10. Back to the **Groups | Naming policy** page, under **Blocked words** section, scroll fown and below **Step 3. Upload your .csv file**, select the **folder** icon to open a file selection window.
11. Browse to **Downloads**, select the **BlockedWords.csv** file and select **Open**.
12. You can see a success message in the upper right of the **Azure Portal**.
13. On the **Group | Naming policy** page, select **Save** to apply the new blocked words setting.
14. Still on the **Groups | Naming policy** page, select the **Group naming policy** tab.
15. Below the **Group naming policy** section, scroll down to **Current policy** and select the checkbox next to **Add prefix**.
16. Select the dropdown textbox below with **Select the type of prefix** and choose **String**.
17. Enter the following to the empty text box: **Group_**
18. Select the checkbox next to **Add suffix.**
19. Select the dropdown textbox and from the drop-down list, choose **Attribute**, and from the drop-down list choose **CountryOrRegion**.
20. On the **Groups - Naming policy** page, under **Current policy** section, preview the group name format listed as **Group_<Group name><CountryOrRegion>**. GroupNaming Policy
21. Select **Save** to apply the new naming policy.
22. Close the browser window.

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 Microsoft 365 Group and Teams names.

9.4.1.7 Task 7 - 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. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Teams web client** at **https://teams.microsoft.com**
3. When the Sign in window is displayed, sign in as **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) using the O365 credentials provided to you.
4. Select **Join or create a team** from the bottom of the teams list.
5. Select **Create team** and **From scratch**.
6. Do not change the Sensitivity dropdown and select **Public**.

7. Enter **Afterwork** below **Team name**.
8. Below the entered name, you can see the configured prefix and suffix for new teams.
9. Select **Create** to create the new team.
10. Select **Skip** to not add any additional members.
11. Review the name of the newly created team.

You have successfully tested the configured naming policy for managing the prefix and suffixes of user created teams. Continue with the next task.

9.4.1.8 Task 8 – Reset Azure AD settings

You can revert any changes in Azure AD unified groups settings to the defaults again. You can do this by loading a blank template and replacing the current configuration with the template. To clean up your test environment after testing, you will now do this and reset all changes you did for Microsoft 365 Groups and Teams.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right click the **Start** button and then select **Windows PowerShell**.
3. Connect to the Azure AD in your tenant with the following cmdlet:

   ```
   Connect-AzureAD
   ```

4. When the Sign in window is displayed, sign in as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) using the O365 credentials provided to you.
5. To load the unifed group template, use the following cmdlet:

   ```
   $Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq "Group.Unified"}
   ```

6. Create a blank Azure AD tenant settings object:

   ```
   $Setting = $Template.CreateDirectorySetting()
   ```

7. Check the Azure AD tenant settings configured in the template:

   ```
   $Setting.Values
   ```

8. Review the current configured Azure AD tenant settings for unified groups and note the differences to the values in the ”$Setting” variable, that contains the default template settings:

   ```
   (Get-AzureADDirectorySetting).Values
   ```

9. Because you will still need the sensitivity labels at a later point of this lab, activate only them in your settings variable again by using the following command:

   ```
   $Setting["EnableMIPLabels"] = "True"
   ```

10. Apply the settings variable to your current configuration to revert all other changes:

    ```
    Set-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where -Property DisplayName -Value
    ```

11. Review your configured Azure AD tenant settings again, which are all on default again:

    ```
    (Get-AzureADDirectorySetting).Values
    ```

12. Close the PowerShell window.

You have successfully reset all Azure AD tenant settings for Microsoft 365 Groups and Teams in your test tenant.

9.4.2 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.

9.4.2.1 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 blocks documents that contain malware.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Microsoft 365 Security center**: **https://security.microsoft.com**.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. In the **Microsoft 365 Security center**, in the left navigation pane, select **Policies& rules**.
5. On the **Policies & rules** page, select **Threat policies**.
6. On the **Threat policies** page, scroll to the **Policies** section and select **Safe Attachments**.
7. On the **Safe Attachments** page, select **Global settings** on the ribbon. If you cannot see **Global settings** select **...** first.
8. In the wizard, set **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams** to **On**.
9. Select the **Save** button.
10. Close the Edge browser windows.

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

9.4.3 Exercise 3: Implement compliance for Microsoft Teams

Before deploying Microsoft Teams in your organization, you need to evaluate Microsoft Teams compliance features to meet organizations requirements. First, you will configure retention settings on data in Microsoft Teams. Next you will configure DLP policy that will search for GDPR related and credit card data and test a DLP policy in the end.

9.4.3.1 Task 1 - 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 last modification.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft 365 compliance center** at **https://compliance.microsoft.com/**.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. In **Office 365 Compliance center**, on the left navigation pane, select **policies**, scroll down to **Data** and select **Retention**.
5. On the **Retention** page, select **New retention policy** to open the **Create retention policy wizard.**
6. On the **Name your policy** page, enter the following and select **Next**:
   - **Name**: Sales retention policy
   - **Description**: Retention policy for Sales department that will retain channel messages for 7 years.
7. On the **Choose locations to apply the policy** page, configure the following settings:
   - **Exchange email**: Off
   - **SharePoint sites**: Off
   - **OneDrive accounts**: Off

- **Office 365 groups**: Off
- **Skype for Business**: Off
- **Exchange public folders**: Off
- **Teams channel messages**: On
- **Teams chats**: Off

8. Select **Edit** right from **Teams channel messages** to open the right-side pane.
9. Select the checkbox left from **Sales** and select **Done**.
10. Select **Next**
11. On the **Decide if you want to retain content, delete it, or both** page, select **Next**.
12. On the **Review and finish** page, review your settings and select **Submit**.
13. Select **Done**. Leave the browser open for the next task.

In this 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**.

9.4.3.2 Task 2 - Create a new retention policy to delete content

After configuring a retain policy to protect data from deletion, you also need to evaluate the capabilities of retention policies to delete content automatically. For demonstration purpose, 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in to the **Microsoft 365 Compliance center**, as **MOD Administrator** in the **Information governance** section and on the **Retention** tab.
3. Select **New retention policy** to open the **Create retention policy wizard.**
4. On the **Name your policy** page, enter the following and select **Next**:
   - **Name**: Teams Rollout deletion policy
   - **Description**: Retention policy for the Teams Rollout team to delete messages older than a day.
5. On the **Choose locations to apply the policy** page, configure the following settings and select **Next**:
   - **Exchange email**: Off
   - **SharePoint sites**: Off
   - **OneDrive accounts**: Off
   - **Office 365 groups**: Off
   - **Skype for Business**: Off
   - **Exchange public folders**: Off
   - **Teams channel messages**: On
   - **Teams chats**: Off
6. Select **Edit** right from **Teams channel messages** to open the right-side pane.
7. Select the checkbox left from **Teams Rollout** and select **Done**.
8. Select **Next**
9. On the **Decide if you want to retain content, delete it, or both** page, select **Only delete items when they reach a certian age** with the following information and then select **Next**:
   - **Delete items older than**: 1 days
   - **Delete the content based on**: when it was created
10. On the **Review and finish** page, review your settings and select **Submit**.

11. 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.

9.4.3.3 Task 3 – 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 policies effect.

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
3. Select the **Teams Rollout** team and the **General** channel.
4. Select **New conversation** from the lower end of the main window.
5. 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.

9.4.3.4 Task 4 - Create a DLP policy for GDPR (PII) content from a template

According to your organization 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 email to 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft 365 compliance center** at **https://compliance.microsoft.com/**.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. In **Microsoft 365 compliance center**, on the left navigation pane, select **Show all** from the bottom of the navigation pane and then select **Data loss prevention**.
5. On the **Data loss prevention** page, select **+ Create policy**.
6. On the **Start with a template or create a custom policy** page, select the **Search for specific templates** search box and type: **GDPR**. The **General Data Protection Regulation (GDPR)** template will be preselected.
7. Select **Next**
8. On the **Name your DLP policy** page, change the default values to the following and select **Next**:
   - **Name**: GDPR DLP Policy
   - **Description**: Data loss prevention policy for GDPR regulations in Teams.
9. On the **Choose locations to apply the policy** page, apply the following selection and select **Next**:
   - **Exchange email**: Off

- **SharePoint sites**: Off
- **OneDrive accounts**: Off
- **Teams chat and channel messages**: On
- **Microsoft Cloud App Security**: Off

10. On the **Define policy settings** page, stay with the default selection from the template **Review and customize default settings from the template** and select **Next**.
11. On the **Info to protect** page, leave the default settings and select **Next**.
12. On the **Protection actions** page, 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 for **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 for **Restrict access or encrypt the content**
13. On the **Customize access and override settings** page, 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 accessing shared SharePoint, OneDrive, and Teams content**.
    - Select **Block only people outside your organization. Users inside your organization will continue to have access**.
    - Select **Override the rule automatically if they report it as false positive**.
14. On the **Test or turn on the policy** page, select **Yes, turn it on right away** and select Next.
15. On the Review your settings page, review your settings, select **Submit** then **Done**.
16. 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.

9.4.3.5 Task 5 - 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in to the **Microsoft 365 Compliance center**, as **MOD Administrator** in the **Data loss prevention** section and on the **Policies** tab.
3. In **Microsoft 365 compliance center**, on the left navigation pane, select **Show all** and then select **Data loss prevention**.
4. On the **Data loss prevention** page, select **+ Create policy**.
5. Select **Custom** and **Custom policy** below **Categories** and **Templates**, to create a blank policy and select **Next**.
6. On the **Name your policy** page, type the following values, and then select **Next**:
    - **Name**: Credit card data DLP Policy
    - **Description**: Data loss prevention policy for credit card data in Teams.

7. On the **Choose locations to apply the policy** page, apply the following selection and select **Next**:
    - **Exchange email**: Off
    - **SharePoint sites**: Off
    - **OneDrive accounts**: Off
    - **Teams chat and channel messages**: On
    - **Microsoft Cloud App Security**: Off
8. Leave the radio button selection unchanged on the **Define policy settings** page and select **Next**.
9. Select **+ Create rule** and enter the following information:
    - **Name**: Credit card numbers found
    - **Description**: Basic rule for protecting credit card numbers form being shared in Teams.
10. Below **Conditions**, select **+ Add condition** and **Content contains**.
11. Leave the group name of **Default**, select **Add** and **Sensitive information types**.
12. From the right-side pane, check the box left of **Credit Card Number** and select **Add**.
13. Leave the high **Accuracy** of 85 to 100 unchanged and do not change the **Instance count** of 1.
14. Below **Action**, select **+ Add an action** and **Restrict access or encrypt content in Microsoft 365 locations**.
15. Select the checkbox of **Restrict access or encrypt content in Microsoft 365 locations** again and select **Block everyone. Only the content owner, the last modifier and the site admin will continue to have access.**
16. Below **User notification**, select the slider to **On** and select **Customize the policy tip text**.
17. Enter the following text to the textbox: **Credit card numbers are not allowed to be shared!**
18. Below **Incident reports**, select the slider **Send an alert to admins when a rule match occurs** and select **Add or remove people**.
19. On the **Add or remove people** page, select the checkbox left from **Joni Sherman** and select **Add**.
20. Select **Save**.
21. Review the rule settings and select **Next**.
22. Select the radio button **Yes, turn it on right away** and select **Next**.
23. Review the policy settings again and select **Submit** then **Done**.
24. Leave the browser open.

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

9.4.3.6 Task 6 – 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 steps does not work, continue with the lab, and perform task 6 at a later point of working through this lab.

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
3. In the left-hand navigation pane, select **Teams**, and then select the **General** channel below **Teams Rollout**.
4. Select **New conversation** from the main window.
5. Enter the following lines to the textbox:
    - MasterCard: 5105105105105100

- Visa: 4111111111111111
- Visa: 4012888888881881

6. Select the arrow to the right from the lower-right corner below the text box to send the message.
7. 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.
8. 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.**
9. Connect to the **Client 1 VM** with the credentials that have been provided to you.
10. You should still be logged in to the **Microsoft 365 Compliance center**. If not, open Microsoft Edge, maximize the browser, and navigate to the **Microsoft 365 Compliance center**: **https://compliance.microsoft.com**.
11. Select **Reports** from the left-hand navigation pane and scroll down to **Organizational data**.
12. Below **DLP Policy Matches** and **DLP Incidents**, you can now see the DLP policy matches. Select **DLP Policy Matches** to open the detailed view.
13. 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.

9.5 END OF LAB

9.6 lab: title: 'Lab 02: Configure security and compliance for teams and content' module: 'Module 2: Implement Microsoft Teams Governance, Security and Compliance'

10 Lab 02: Configure Security and Compliance for teams and content

11 Student lab manual

11.1 Lab Scenario

In the labs of this course you will assume the role of the System Administrator for Contoso Ltd. Your organization is planning to deploy Microsoft Teams. Before starting the deployment, IT department is gathering business requirements about Teams governance as well as data security and compliance, including how the data shared in Teams is regulated according to the organization's compliance requirements. After you complete the planning process, you will configure Microsoft 365 Groups governance, protect Teams from threats, and configure Teams to meet your organization compliance requirements.

11.2 Objectives

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

- Activate, create and assign sensitivity labels
- Configure expiration policies
- Restrict creation of new teams to members of a security group
- Create naming policies
- Reset all Azure AD settings to defaults
- Activating Safe Attachments protection for SharePoint, OneDrive and Teams
- Create, configure and test retention policies
- Create and test a DLP policy to protect GDPR content

11.3 Lab Setup

- **Estimated Time:** 90 minutes.

11.4 Instructions

11.4.1 Exercise 1: Implement governance and lifecycle management for Microsoft Teams

Your organization has started the planning process for Microsoft 365 services adoption. You are assigned as 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, configuring and assigning sensitivity labels, creating Microsoft 365 groups expiration policies, configuring Microsoft 365 Group creation policy permissions, and configuring with testing Microsoft 365 Groups naming policies.

11.4.1.1 Task 1 – Activate sensitivity labels for Teams

You need to evaluate governance for Microsoft 365 Groups before deploying them in your organizations. In this task, you will activate the sensitivity labels for Teams in Azure AD, for being able to assign labels in a following task.

1. Open a **Windows PowerShell** window.
2. Install the Azure AD Preview module:

   Install-Module AzureADPreview

3. Connect to Azure AD in your tenant as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com):

   Connect-AzureAD

4. Load the Azure AD unified group template:

   ```
   $Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq "Group.Unified"}
   ```

5. Check if a Azure AD setting is already existing and load it, if yes. If not, create a blank Azure AD setting object. Run the following cmdlet to populate the "$Setting" variable:

   ```
   if (!($Setting=Get-AzureADDirectorySetting|Where {$_.TemplateId -eq $Template.Id})) {$Setting = $T
   ```

6. Enable the Microsoft Identity Protection (MIP) support:

   ```
   $Setting["EnableMIPLabels"] = "True"
   ```

7. To verify the new configuration, run the following cmdlet:

   ```
   $Setting.Values
   ```

8. As soon as the "Setting" variable attributes contain the desired values, write back the settings object to your directory. Use the following cmdlet, to create a new "Group.Unified" Azure AD configuration with the custom settings:

   ```
   New-AzureADDirectorySetting -DirectorySetting $Setting
   ```

   Note: Since this is a new tenant, there's no directory settings object in the tenant yet. You need to use `New-AzureADDirectorySetting` to create a directory settings object at the first time.

   If there's an existing directory settings object, you will need to run the following cmdlet to update the directory setting in Azure Active Directory:

   ```
   Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
   ```

9. Close the PowerShell window.

You have successfully changed your tenants Azure AD settings and activated sensitivity labels for Microsoft 365 Groups and Microsoft Teams.

11.4.1.2 Task 2 - Create sensitivity labels for Teams

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

1. Sign in to the **Microsoft 365 compliance center** **https://compliance.microsoft.com** using the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Turn on now the ability to process content in Office online files that have encrypted sensitivity labels applied.
3. Create a new sensitivity label with the following settings:
   - **Name**: General
   - **Display name**: General
   - **Description for users**: General information without protection
   - **Description for admins**: General information without encryption, marking or sharing restriction settings activated
   - **Privacy:** None. Team and group members can set the privacy settings themselves
   - **External users access**: Select Let Microsoft 365 group owners add people outside the organization to the group
   - **Unmanaged devices:** Allow full access from desktop apps, mobile apps, and the web
4. Create the second new sensitivity label with the following settings:
   - **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
   - **Assign permissions now or let users decide**: Assign permissions now
   - **User access to content expires**: Never
   - **Allow offline access**: Always
   - **Assign permissions**: Add all users and groups in your organization
   - **Watermark text**: Internal use only
   - **Privacy:** None. Team and group members can set the privacy settings themselves
   - **External users access**: Leave the box unchecked
   - **Unmanaged devices:** Allow limited, web-only access
5. Create the third new sensitivity label with the following settings:
   - **Name**: Confidential
   - **Display name**: Confidential
   - **Description for users**: Confidential information with all protection
   - **Description for admins**: Confidential information with all restrictive encryption, marking, and sharing settings activated
   - **Assign permissions now or let users decide**: Assign permissions now
   - **User access to content expires**: Never
   - **Allow offline access**: Never
   - **Assign permissions**: Add all users and groups in your organization
   - **Choose permissions**: Reviewer
   - **Watermark text**: Confidential
   - **Privacy:** Private. Only team owners and members can access the group or team, and only owners can add members
   - **External users access**: Leave the box unchecked

- **Unmanaged devices:** Allow limited, web-only access

6. Publish the sensitivity labels with the following settings:
   - **Name**: All company sensitivity labels
   - **Description**: Default sensitivity labels for all users in the company
   - Publish to all users and groups
   - **Default to documents and email**: General
   - **Default to groups and sites**: General
7. Close the **Microsoft 365 compliance center**

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.

11.4.1.3 Task 3 - 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. Connect to a client and sign in to the Teams Desktop client using **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft
2. Assign the **Internal** sensitivity label to the **Teams Rollout** team.
3. Close the Teams Desktop client.

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

11.4.1.4 Task 4 - Create and assign an expiration policy

Based on the organization 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. Sign in to the **Azure Portal** https://portal.azure.com using the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Go to **Azure Active Directory** and **Groups**.
3. On the **Groups** page, configure **Expiration** so that **Group lifetime (in days)** is **90**.
4. In the **Email contact for groups with no owners** field, type the email address (JoniS@<YourTenant>.onmicrosoft.co
5. Apply the expiration policy you just created to **Teams Rollout** group only.

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

11.4.1.5 Task 5 - Configure a group creation policy

You are an administrator for your Teams 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. Open a **Windows PowerShell** window.
2. Connect to the Azure AD in your tenant as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com):

   ```
   Connect-AzureAD
   ```

3. Create a new security group "GroupCreators" by running the following cmdlet:

   ```
   New-AzureADGroup -DisplayName "GroupCreators" -SecurityEnabled:$true -MailEnabled:$false -MailNickl
   ```

4. Run following cmdlet to add **Lynne Robbins** to the new security group:

```
Get-AzureADGroup -SearchString "GroupCreators" | Add-AzureADGroupMember -RefObjectId (Get-AzureADU
```

5. Fetch the current group settings for the Azure AD organization

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where -Property DisplayN
```

6. Run following cmdlet to modify the group creation setting for your tenant with the "EnableGroupCreation" attribute:

```
$Setting["EnableGroupCreation"] = "False"
```

7. Run following cmdlet to add the just created security group "GroupCreators" as permitted group to create groups, by their ObjectID:

```
$Setting["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString "GroupCreators").objecti
```

8. Then save the changes and apply the settings:

```
Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
```

9. To test the newly configured settings, connect to the **Client 2 VM** with the credentials that have been provided to you.
10. In Microsoft Edge browser, sign in to **Microsoft Teams web client** (**https://teams.microsoft.com/**) as user MeganB@<YourTenant>.OnMicrosoft.com.
11. Select **Join or create a team** and you won't see the option to **Create team**.
12. Close all open windows.

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

11.4.1.6 Task 6 - 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 letters **Group** and end with the **Country** attribute. Furthermore, there is an internal regulation that forbids using following specific keywords in Teams names: CEO, Payroll and HR.

1. Sign in to the **Azure Portal** (**https://admin.microsoft.com**) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Go to **Azure Active Directory** and **Groups**.
3. On the **Groups** page, configure the **Naming policy**.
4. Download a blocked words sample file. Save the file, and then open the file in **Notepad**.
5. Type **CEO, Payroll,** HR, replacing the empty quotes in the Notepad window and save the file in place. Afterwards, close the Notepad file.
6. Back to the **Groups | Naming policy** page, upload the **BlockedWords.csv** file you just created.
7. On the **Groups | Naming policy** page, configure group name prefix to be the string: **Group_**, and the group name suffix to be the **CountryOrRegion** attribute.
8. On the **Groups | Naming policy** page, under **Current policy** section, preview the group name format listed as **Group_<Group name><CountryOrRegion>**. GroupNaming Policy.
9. Select **Save** to apply the new naming policy.

In this task, you have configured a naming policy that will block specific words to be used in an Microsoft 365 Group name, as well as you have configured a new naming policy for Microsoft 365 Group and Teams names.

11.4.1.7 Task 7 - 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. Sign in to the Teams web client (**https://teams.microsoft.com**) using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
2. Create a new team with the name **Afterwork** with no members.
3. Review the name of the newly created team.

You have successfully tested the configured naming policy for managing the prefix and suffixes of user created teams. Continue with the next task.

11.4.1.8 Task 8 – Reset Azure AD settings

You can revert any changes in Azure AD unified groups settings to the defaults again. You can do this by loading a blank template and replacing the current configuration with the template. To clean up your test environment after testing, you will now do this and reset all changes you did for Microsoft 365 Groups and Teams.

1. Open a regular **Windows PowerShell** window.
2. Connect to the Azure AD in your tenant as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com):

   ```
   Connect-AzureAD
   ```

3. To load the unifed group template, use the following cmdlet:

   ```
   $Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq "Group.Unified"}
   ```

4. Create a blank Azure AD tenant settings object:

   ```
   $Setting = $Template.CreateDirectorySetting()
   ```

5. Check the Azure AD tenant settings configured in the template:

   ```
   $Setting.Values
   ```

6. Check the current configured Azure AD tenant settings and note the differences, to the values in the ”$Setting” variable, that contains the default template settings:

   ```
   (Get-AzureADDirectorySetting).Values
   ```

7. Because you will still need the sensitivity labels at a later point of this lab, activate only them in your settings variable again:

   ```
   $Setting["EnableMIPLabels"] = "True"
   ```

8. Apply the configured settings, to revert all other changes:

   ```
   Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
   ```

9. Check your configured Azure AD tenant settings again, which are all on default again:

   ```
   (Get-AzureADDirectorySetting).Values
   ```

10. Close the PowerShell window.

You have successfully reset all Azure AD tenant settings for Microsoft 365 Groups and Teams in your test tenant.

11.4.2 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.

11.4.2.1 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 blocks documents that contain malware.

1. Sign in to the **Microsoft 365 security center** (https://security.microsoft.com) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. In the **Microsoft 365 security center**, navigate to **Policies& rules** and open **Safe Attachments**.
3. On the **Safe Attachments** page, select **Global settings** then set **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams** to **On**.
4. Select **Save** and close the Edge browser window.

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

11.4.3 Exercise 3: Implement compliance for Microsoft Teams

Before deploying Microsoft Teams in your organization, you need to evaluate Microsoft Teams compliance features to meet organizations requirements. First, you will configure retention settings on data in Microsoft Teams. Next you will configure DLP policy that will search for GDPR related and credit card data and test a DLP policy in the end.

11.4.3.1 Task 1 - Create a new retention policy to retain content

Teams retention settings are very important for managing the lifecycle of company data, and 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 last modification.

1. Sign in to the **Microsoft 365 compliance center** (https://compliance.microsoft.com) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Navigate to **policies**, **Data** and **Retention**.
3. On the **Retention** page, create a new retention policy with the following configuration:
   - **Name**: Sales retention policy
   - **Description**: Retention policy for Sales department that will retain channel messages for 7 years
   - **Locations to apply to policy:** Teams channel messages > **Sales** team only
   - **Retain items for a specified period:** 7 years from the date the item was last modified
   - **At the end of the retention period**: Do nothing
4. Leave the browser open for the next task.

In this 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**.

11.4.3.2 Task 2 - Create a new retention policy to delete content

After configuring a retain policy to protect data from deletion, you also need to evaluate the capabilities of retention policies to delete content automatically. For demonstration purpose, 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. Sign in to the **Microsoft 365 compliance center** (https://compliance.microsoft.com) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Navigate to **policies**, **Data** and **Retention**.
3. On the **Retention** page, create a new retention policy with the following configuration:
   - **Name**: Teams Rollout deletion policy.
   - **Description**: Retention policy for the Teams Rollout team to delete messages older than a day.

- Delete content that's older than **1 day** from the date **when it was created.**
- **Locations to apply to policy:** Teams channel messages > Teams Rollout team only.

4. Close all browser windows.

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.

11.4.3.3 Task 3 – 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 policies effect.

1. Connect to a client and sign in to the Teams Desktop client using **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft
2. Create a **New conversation** in the **General** channel of **Teams Rollout.**
3. Write down **Hello world!** and any other messages you like.
4. 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.

11.4.3.4 Task 4 - Create a DLP policy for GDPR (PII) content from a template

According to your organization 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 email to 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. Sign in to the **Microsoft 365 compliance center** (https://compliance.microsoft.com) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. Navigate to **Data loss prevention**.
3. Create a new DLP policy with the following configuration:
   - **Template:** General Data Protection Regulation (GDPR)
   - **Name:** GDPR DLP Policy
   - **Description:** Data loss prevention policy for GDPR regulations in Teams
   - **Locations to apply to policy:** Teams chat and channel messages
   - **Instances of the same sensitive info type**: 1
   - **Send incident reports in email**: MOD Administrator and Joni Sherman
   - Select **Block people from sharing and restrict access to shared locations**
   - Select **Only people outside your organization. People inside your organization will continue to have access**
   - Select **Override the rule automatically if they report it as false** positive
   - **Test or turn on the policy:** Turn it on right away
4. Stay on the **Data loss prevention page** in the **Microsoft 365 compliance center**.

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.

11.4.3.5 Task 5 - 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. Sign in to the **Microsoft 365 compliance center** (https://compliance.microsoft.com) using **MOD Administrator** (admin@<*YourTenant*>.onmicrosoft.com).
2. Navigate to **Data loss prevention**.
3. Create a new DLP policy with the following configuration:
   - **Template**: Custom
   - **Name:** Credit card data DLP Policy
   - **Description**: Data loss prevention policy for credit card data in Teams
   - **Locations to apply to policy:** Teams chat and channel messages
   - **Custom rule name**: Credit card numbers found
   - **Custom rule description**: Basic rule for protecting credit card numbers form being shared in Teams
   - **Conditions**: Content contains at least 1 instance of Sensitive information type "Credit Card Number" with default accuracy
   - **Action**: Restrict access or encrypt content in Microsoft 365 locations
   - **User notification**: Customize the policy tip text: "Credit card numbers are not allowed to be shared!"
   - **Incident reports**: Send an alert to admins when a rule match occurs and include Joni Sherman
   - **Test or turn on the policy** Turn it on right away
4. Close the **Data loss prevention page** and the **Microsoft 365 compliance center**.

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

11.4.3.6 Task 6 – 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 steps do not work, continue with the lab, and perform task 6 at a later point of working through this lab.

1. Connect to a client and sign in to the Teams Desktop client using **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft
2. Create a **New conversation** in the **General** channel of **Teams Rollout.**
3. Enter the following lines to the textbox and send the message:
   - MasterCard: 5105105105105100
   - Visa: 4111111111111111
   - Visa: 4012888888881881
4. Review the error message.
5. Sign in to the **Microsoft 365 compliance center** (https://compliance.microsoft.com) using **MOD Administrator** (admin@<*YourTenant*>.onmicrosoft.com).
6. Navigate to **Reports**.
7. Review the DLP policy violations.

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

11.5 END OF LAB

11.6 lab: title: 'Lab 03: Plan and configure network settings for Microsoft Teams ' type: 'Answer Key' module: 'Module 3: Prepare the environment for a Microsoft Teams deployment'

12 Lab 03: Plan and configure network settings for Microsoft Teams

13 Student lab answer key

13.1 Use the new Microsoft 365 admin center

Throughout the lab exercises for this course, if you navigate to the Microsoft 365 admin center and are prompted with a window asking if you want to try the new Microsoft 365 admin center, always select the **Try it now** button.

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

13.2 Lab Scenario

In the labs of this course you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. Your organization is planning to deploy Microsoft Teams. However, there are concerns about 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. Furthermore, your organization is planning to purchase and deploy multiple Teams devices. You will need to evaluate different devices profiles and configure profile settings for the devices. At the end, you will need to evaluate the process of creating Microsoft Teams room, where multiple Teams rooms will be purchased in your organization.

13.3 Objectives

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

- Calculate the network bandwidth capacity for a Teams deployment
- Work with the Network Testing Companion on a client
- Create configuration profiles for devices
- Configure a new Microsoft Teams Room

13.4 Lab Setup

- **Estimated Time:** 60 minutes.

13.5 Instructions

13.5.1 Exercise 1: Calculate networking capabilities

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 reliable network connection. Therefore, it is very important that Teams admins have tools that could help to estimate the bandwidth consumption according to specific business requirements and existing network infrastructure and provide best experience to business users.

13.5.1.1 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:

Location	Total number of employees	WAN link capacity / audio/video queue size (Mbps)	Offic
New York HQ	1000	1000/300/500	Expre
Los Angeles Office	250	500/100/200	Remo
Houston Office	150	400/50/100	Remo

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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Sign in to the **Teams admin center** (**https://admin.microsoft.com**) using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. In the **Teams admin center,** on the left-hand navigation pane, expand **Planning**, and select **Network Planner**.
4. On the **Network planner** page, under **Network plans** tab, select **Add**.
5. On the **Network plan name** page, in the **Network plan name** box, type **Contoso plan**, and in the **Description** box type **Contoso Teams Network plan**, and then select **Apply**.
6. On the **Network planner** page, select **Personas** tab, and then select **Add**.
7. On the **Add persona** page, in the **Persona name** box type **New York office**, in the **Description** box type **New York office Teams users**, under the **Permissions** section, turn **On** all buttons, and then select **Apply**.
8. Select **Add** again, and on the **Add persona** page, in the **Persona name** box type **Los Angeles office**, in the **Description** box type **Los Angeles office Teams users**, under the **Permissions** section, turn **Off PSTN** button, and turn **On** all other buttons, and then select **Apply**.
9. Select the **Networks plans** tab, then select **Contoso plan**, and under **Network sites** tab, select **Add a network site**.
10. On the **Network site** page, enter the following information:
    - In the **Network site name** field, type **New York HQ site**.
    - In the in the description field type **New York HQ site network infrastructure**.
    - In the **Network users** field type **1000**.
    - In the **Network settings** section, in the **Subnet** box type **172.16.0.0**, and in the **Network range** box type **16**.
    - In the **Network settings** section, turn **On** the **Express Route** button.
    - In the **Network settings** section, in the **Internet link capacity** box, type **1000**.
    - In the **Network settings** section, in the **PSTN egress** drop-down box, choose **Use VoIP only**, and then select **Save**.
11. On the **Contoso plan** page, under **Network sites** tab, select **Add a network site**.
12. On the **Network site** page, enter the following information:
    - In the **Network site name** field, type **Los Angeles site**.
    - In the in the description field type **Los Angeles site network infrastructure**.
    - In the **Network users** field type **250**.
    - In the **Network settings** section, in the **Subnet** box type **192.168.10.0**, and in the **Network range** box type **24**.
    - In the **Network settings** section, ensure **ExpressRoute** button is **Off**.

- In the **Network settings** section, turn **On** the **Connected to WAN** button, then in **WAN link capacity** box type **500**, in the **WAN audio queue size** box type **100**, and in **Video queue size** box type **200**.
- In the **Network settings** section, in the **PSTN egress** drop-down box, **choose VoIP only**, and then select **Save**.

13. On the **Contoso plan** page, under **Network sites** tab, select **Add a network site**.
14. On the **Network site** page, enter the following information:
    - In the **Network site name** field, type **Houston site**.
    - In the in the description field type **Houston site network infrastructure**.
    - In the **Network users** field type **150**.
    - In the **Network settings** section, in the **Subnet** box type **192.168.20.0**, and in the **Network range** box type **24**.
    - In the **Network settings** section, ensure ExpressRoute button is **Off**.
    - In the **Network settings** section, turn **On** the **Connected to WAN** button, then in **WAN link capacity** box type **400**, in the **WAN audio queue size** box type **50**, and in **Video queue size** box type **100**.
    - In the **Network settings** section, in the **PSTN egress** drop-down box, **choose VoIP only**, and then select **Save**.
15. On the **Contoso plan** page, select **Report** tab and then select **Start a report**.
16. On the Report page, in the **Report name** field, type **Contoso report,** and in the description field, type **Contoso network estimation report**.
17. Under the **Calculation** section, review the default distribution of different personas in each site, and then select **Generate report**.
18. Under the **Reports** section, review the impact of Microsoft Teams on the Contoso network infrastructure by analyzing the report results on bandwidth needed for audio, video, screen sharing, Office 365 traffic, and PSTN.
19. On the report page, select the **Switch to chart view** at 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 impact 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.

13.5.1.2 Task 2 - Use network testing companion

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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right click the **Start** button and then select **Windows PowerShell (Admin)**.
3. Confirm the **User Account Control** window with **Yes**.
4. In the PowerShell window, enter the following cmdlet to install the Network Testing Companion:

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

5. Type in **y** and hit **return** for the Question with the **Untrusted repository**.

6. Enter the following cmdlet to create desktop shortcuts:

   ```
   Invoke-ToolCreateShortcuts
   ```

7. Close the PowerShell window.
8. Open **Network Testing Companion** from the desktop shortcut and select the **Install** button, to install the Network Assessment Tool.
9. On the **User Account Control** window, select **Yes**.
10. Wait until window **Skype for Business and Microsoft Teams Network Testing Companion** initializes with green **Start** button appears in the **Network Connectivity and Quality Test** section on the right side of the window.
11. Review the information under **Windows operating system** and **Internet connection** sections and verify that no errors appear.
12. Select the green **Install** circle below **Network connectivity and quality test**.
13. A **User Account Control** window will appear in the taskbar. Maximize it and select **Yes.**
14. When the installation was successful, the symbol below **Network assessment tool** will change to a green checkmark in a circle too.
15. Select the green **Start** button in the **Network Connectivity and Quality Test** section to start the tests.
16. On the **Windows Security Alert** window, select **Allow access**.

    > **Note:** If you receive a timeout message during the connectivity test, you can select the **Settings** tab in the tool. Adjust the **Connectivity test timeout (seconds)** option to a larger value and then start the test again.

17. When the tests have finished, the symbols below **Connectivity** and **Quality** will turn to green checkmarks in green circles.
18. After the test is **finished**, select the **View Results** tab and review the detailed results of the tests.
19. In the **View Results** tab, select **Report** file icon under **Network Connectivity** and **Network Quality** and review the testing steps and reports.
20. Discuss the results with the instructor.
21. Close all notepad windows and the **Skype for Business and Microsoft Teams Network Testing Companion.**

In this task, you have used Skype for Business and Microsoft Teams Network Testing Companion to test the connectivity and connection quality of your network infrastructure for Microsoft Teams.

13.5.2 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 complete meeting experience with HD video, audio, and content sharing in conference rooms. You will need to prepare the deployment prerequisites by define Microsoft Teams Rooms service account in Office 365.

13.5.2.1 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 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Teams admin center** at **https://admin.teams.microsoft.com/**.

3. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. In **Teams admin center**, on the left navigation pane, select **Devices**, and then choose **IP Phones**.
5. On the **IP Phones** page, select **Configuration profiles** tab, and then select **Add**.
6. 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**
7. 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)**
8. 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**
9. Under **Network settings**, configure following settings:
   - DHCP enabled: **On**
   - Logging enabled: **Off**
   - Device's default admin password: **Pass@word1**
10. Once you complete with the configuration profile settings, select **Save**.

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

13.5.2.2 Task 2 - Create a Microsoft 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. Because you need to use the Exchange Online PowerShell to complete this task, you will first install the new Exchange PowerShell module.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right click the **Start** button and then select **Windows PowerShell (Admin)**.
3. Confirm the **User Account Control** window with **Yes**.
4. Enter the following cmdlet to install the Exchange PowerShell v2:

   ```
   Install-Module ExchangeOnlineManagement
   ```

5. Confirm the Untrusted repository message with **y** for yes.
6. Close the elevated PowerShell window.
7. Right-click the Start button and select **Windows PowerShell.**

8. Enter the following cmdlet to connect to Exchnage Online PowerShell:

   ```
   Connect-ExchangeOnline
   ```

9. When you see the **Sign in** window, enter admin@<YourTenant>.onmicrosoft.com and sign in with the credentials provided to you.

10. Create a new room mailbox named **NY-TeamsRoom1** by running the following cmdlet (remember to replace your tenant name):

    ```
    New-Mailbox -Name "NY-TeamsRoom1" -Alias NY-TeamsRoom1 -Room -EnableRoomMailboxAccount $true -Micr
    ```

11. Configure the Calendar Processing features for the Teams Room. Read the following description and run the cmdlet at the end:

    - AutomateProcessing: **AutoAccept** (Meeting organizers receive the room reservation decision directly without human intervention: free = accept; busy = decline.)
    - AddOrganizerToSubject: **$false** (The meeting organizer is not added to the subject of the meeting request.)
    - DeleteComments: **$false** (Keep any text in the message body of incoming meeting requests.)
    - DeleteSubject: **$false** (Keep the subject of incoming meeting requests.)
    - RemovePrivateProperty: **$false** (Ensures the private flag that was sent by the meeting organizer in the original meeting request remains as specified.)
    - AddAdditionalResponse: **$true** (The text specified by the AdditionalResponse parameter is added to meeting requests.)
    - AdditionalResponse: **"This is a Teams Meeting room"** (The additional text to add to the meeting request.)

    ```
    Set-CalendarProcessing -Identity "NY-TeamsRoom1" -AutomateProcessing AutoAccept -AddOrganizerToSub
    ```

12. Disconnect from Exchage Online and end the established session with the following cmdlet:

    ```
    Disconnect-ExchangeOnline
    ```

13. Confirm the command with **y** for yes.

14. Connect to **Azure AD PowerShell** to configure Teams Room account settings by running the following cmdlets:

    ```
    Connect-AzureAD
    ```

    When you see the Sign in window, type admin@<YourTenant>.onmicrosoft.com and sign in with the credentials provided to you.

15. Disable the password expiration for the Teams Room account **NY-TeamsRoom1** by running the following cmdlet:

    ```
    Get-AzureADUser | Where {$_.DisplayName -eq "NY-TeamsRoom1"} | Set-AzureADUser -PasswordPolicies D
    ```

16. Close the PowerShell window.

17. Open **Microsoft Edge**, maximize the window and navigate to the **Microsoft 365 admin center** at **https://admin.microsoft.com/**.

18. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.

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

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

21. In the results page, locate the **Collaboration and communication** section, and under **Microsoft Teams Rooms Standard** tile, select **Details** and then select **Get free trial**.

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

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

24. Select the NY-TeamsRoom1@<YourTenant>.onmicrosoft.com account, and then select the **Licenses and Apps** tab.
25. In the NY-TeamsRoom1@<YourTenant>.onmicrosoft.com page, under the **Licenses and Apps** tab, select **Microsoft Teams Rooms Standard** and then select **Save changes**.
26. 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.

13.6 END OF LAB

13.7 lab: title: 'Lab 03: Plan and configure network settings for Microsoft Teams' module: 'Module 3: Prepare the environment for a Microsoft Teams deployment'

14 Lab 03: Plan and configure network settings for Microsoft Teams

15 Student lab manual

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.**

15.1 Lab Scenario

In the labs of this course, you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. Your organization is planning to deploy Microsoft Teams. However, there are concerns about 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. Furthermore, your organization is planning to purchase and deploy multiple Teams devices. You will need to evaluate different devices profiles and configure profile settings for the devices. At the end, you will need to evaluate the process of creating Microsoft Teams room, where multiple Teams' rooms will be purchased in your organization.

15.2 Objectives

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

- Calculate the network bandwidth capacity for a Teams deployment
- Work with the Network Testing Companion on a client
- Create configuration profiles for devices
- Configure a new Microsoft Teams Room

15.3 Lab Setup

- **Estimated Time:** 60 minutes.

15.4 Instructions

15.4.1 Exercise 1: Calculate networking capabilities

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 reliable network connection. Therefore, it is very important that Teams admins have tools that could help to estimate the bandwidth consumption according to specific business requirements and existing network infrastructure and provide best experience to business users.

15.4.1.1 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:

Location	Total number of employees	WAN link capacity / audio/video queue size (Mbps)	Offic
New York HQ	1000	1000/300/500	Expre
Los Angeles Office	250	500/100/200	Remo
Houston Office	150	400/50/100	Remo

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.microsoft.com**) using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. In the **Teams admin center,** under **Planning** section, open **Network Planner**.
3. In **Network planner**, create a new network plan named **Contoso plan**, with the description **Contoso Teams Network plan**.
4. In **Network planner**, add a **persona** with name **New York office**, and add a description **New York office Teams users**. Under **Permissions** section, turn **On** all buttons.
5. In **Network planner**, add a **persona** with name **Los Angeles office**, and add a description **Los Angeles office Teams users**. Under **Permissions** section, turn **Off PSTN** button, and turn **On** all other buttons.
6. In **Contoso plan**, add a **Network site** with following configuration:
   - Network site name: **New York HQ site**
   - Description: **New York HQ site network infrastructure**
   - Network users: **1000**
   - In the **Network settings** section, add following configuration:
     - Subnet: **172.16.0.0**, Network range: **16**
     - Express Route: **On**
     - Internet link capacity: **1000**
     - PSTN egress: **Use VoIP only**
7. In **Contoso plan**, add a **Network site** with following configuration:
   - Network site name: **Los Angeles site**
   - Description: **Los Angeles site network infrastructure**
   - Network users field type: **250**
   - In the **Network settings** section, add following configuration:
     - Subnet: **192.168.10.0**, Network range: **24**
     - ExpressRoute: **Off**
     - Connected to WAN: **On**
     - WAN link capacity: **500**
     - WAN audio queue size: **100**

- Video queue size: **200**
- Internet link capacity **500**
- PSTN egress: **Use VoIP only**

8. In **Contoso plan**, add a **Network site** with following configuration:
   - Network site name: **Houston site**
   - Description: **Houston site network infrastructure**
   - Network users: **150**
   - In the **Network settings** section, add following configuration:
     - Subnet: **192.168.20.0**, Network range: **24**
     - ExpressRoute: **Off**
     - Connected to WAN: **On**
     - WAN link capacity: **400**
     - WAN audio queue size: **50**
     - Video queue size: **100**
     - Internet link capacity **400**
     - PSTN egress: **Use VoIP only**
9. Start a report for the **Contoso plan** with a name **Contoso report** and a description **Contoso network estimation report**.
10. Under the **Calculation** section, review the default distribution of different personas in each site, and then select **Generate report**.
11. Under the **Reports** section, review the impact of Microsoft Teams on the Contoso network infrastructure by analyzing the report results on bandwidth needed for audio, video, screen sharing, Office 365 traffic, and PSTN.
12. On the report page, use the **Switch to chart view** 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-30% is the recommended threshold. By changing this value and selecting **Run report**, you can see the different impact 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.

15.4.1.2 Task 2 - Use network testing companion

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. Open an elevated **Windows PowerShell (Admin)** window.
2. Install the Network Testing Companion with the following cmdlet, and accept the question for **Untrusted repository**:

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

3. Create shortcuts for the desktop by running the following cmdlet:

   ```
   Invoke-ToolCreateShortcuts
   ```

4. Open **Network Testing Companion** and then install the Network Assessment Tool, accepting the **User Account Control** dialog.
5. Select the green **Start** button in the **Network Connectivity and Quality Test** section to start the tests.

6. On the **Windows Security Alert** window, select **Allow access**.
7. After the test is **finished**, select the **View Results** tab and review the detailed results of the tests.
8. In the **View Results** tab, select **Report** file icon under **Network Connectivity** and **Network Quality** and review the testing steps and reports.
9. After the test is finished, review the results of the testing with detailed testing steps and reports.
10. Discuss the results with the instructor.
11. Close all notepad windows and the **Skype for Business and Microsoft Teams Network Testing Companion.**

In this task, you have used Skype for Business and Microsoft Teams Network Testing Companion to test the connectivity and connection quality of your network infrastructure for Microsoft Teams.

15.4.2 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 complete meeting experience with HD video, audio, and content sharing in conference rooms. You will need to prepare the deployment prerequisites by define Microsoft Teams Rooms service account in Office 365.

15.4.2.1 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 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. Sign in to the **Teams admin center** **https://admin.teams.microsoft.com** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. In **Teams admin center**, in the **Devices** section, on the **IP Phones** page, create a **Configuration profile** with following configuration:
   - Configuration profile Name: **New York Teams Desk Phones**
   - Description: **Configuration profile for Teams Desk Phones in New York HQ**
3. 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)**
4. 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**
5. Under **Network settings**, configure following settings:
   - DHCP enabled: **On**
   - Logging enabled: **Off**

- Device's default admin password: **Pass@word1**

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

15.4.2.2 Task 2 - Create a Microsoft 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. Because you need to use the Exchange Online PowerShell to complete this task, you will first install the new Exchange PowerShell module.

1. Open an elevated **Windows PowerShell (Admin)** window.
2. Install the Exchange PowerShell v2 using the following cmdlet:

   ```
   Install-Module ExchangeOnlineManagement
   ```

3. Enter the following cmdlet to connect to Exchange Online PowerShell, signing in with **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com):

   ```
   Connect-ExchangeOnline
   ```

4. Create a new room mailbox named **NY-TeamsRoom1** by running the following cmdlet (remember to replace your tenant name):

   ```
   New-Mailbox -Name "NY-TeamsRoom1" -Alias NY-TeamsRoom1 -Room -EnableRoomMailboxAccount $true -Micr
   ```

5. Configure the Calendar Processing features for the Teams Room. Read the following description and run the cmdlet at the end:
   - AutomateProcessing: **AutoAccept** (Meeting organizers receive the room reservation decision directly without human intervention: free = accept; busy = decline.)
   - AddOrganizerToSubject: **$false** (The meeting organizer is not added to the subject of the meeting request.)
   - DeleteComments: **$false** (Keep any text in the message body of incoming meeting requests.)
   - DeleteSubject: **$false** (Keep the subject of incoming meeting requests.)
   - RemovePrivateProperty: **$false** (Ensures the private flag that was sent by the meeting organizer in the original meeting request remains as specified.)
   - AddAdditionalResponse: **$true** (The text specified by the AdditionalResponse parameter is added to meeting requests.)
   - AdditionalResponse: **"This is a Teams Meeting room"** (The additional text to add to the meeting request.)

   ```
   Set-CalendarProcessing -Identity "NY-TeamsRoom1" -AutomateProcessing AutoAccept -AddOrganizerToSub
   ```

6. Disconnect from Exchage Online and end the established session with the following cmdlet:

   ```
   Disconnect-ExchangeOnline
   ```

7. Connect to **Azure AD PowerShell**, signing in with **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com)

   ```
   Connect-AzureAD
   ```

8. Disable the password expiration for the Teams Room account **NY-TeamsRoom1** by running the following cmdlet:

   ```
   Get-AzureADUser | Where {$_.DisplayName -eq "NY-TeamsRoom1"} | Set-AzureADUser -PasswordPolicies D
   ```

9. Close the PowerShell window and sign in to the **Microsoft 365 admin center** **https://admin.microsoft.com** using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
10. In the **Microsoft 365 admin center** from **Purchase services** (under **Billing**), obtain a **Microsoft Teams Rooms Standard** trial license.
11. In the **Microsoft 365 admin center** from **Users** section, choose **Active Users**.

12. Add **Microsoft Teams Rooms Standard** product license to the NY-TeamsRoom1@<YourTenant>.onmicrosoft.com account.

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

15.5 END OF LAB

15.6 lab: title: 'Lab 04: Manage teams' type: 'Answer Key' module: 'Module 4: Deploy and manage teams'

16 Lab 04: Manage teams

17 Student lab answer key

17.1 Lab Scenario

In the labs of this course, you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. 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 the second half of this lab, you will configure the guest access for your tenant and review access for both, internal and external users.

17.2 Objectives

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

- Create a Team from a Microsoft 365 Group
- Create a Team by using PowerShell
- Create a Team by using Microsoft Graph API
- Create a Team with dynamic membership
- Archive and unarchive Teams
- Delete and recover Teams
- Configure guest access in Azure and Teams
- Review Access to a resource

17.3 Lab Setup

- **Estimated Time:** 90 minutes.

17.4 Instructions

17.4.1 Exercise 1: Manage team resources

17.4.1.1 Task 1 - Create a team from an existing Microsoft 365 Group

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

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Select the **Teams** icon on the taskbar to start the Teams Desktop client and sign in as **Joni Sherman** (JoniS@<YourTenant>.OnMicrosoft.com).
3. The Microsoft Teams Desktop client will start. If a **Bring your team together**, or **Get the Teams mobile app** window appears, close both windows.
4. 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.
5. In the **Create a team** dialog , select **From a group or team**.
6. In the **Create a new team from something you already own** dialog, select **Microsoft 365 group**.

7. 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.
8. Select the three dots (**...**) right from the new team in the left pane and select **Manage team**.
9. Check, if **Joni Sherman** is still listed below Owners.
10. Select **Members and guests** and check that following members are still listed: **Lynne Robbins**, **Megan Bowen**, **Allan Deyoung** and **Alex Wilber**.
11. Select the **General** channel below the **IT-Department** teams.
12. Close the Teams Desktop client.

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.

17.4.1.2 Task 2 - Create a team by using PowerShell

In this task you will create via the Teams PowerShell a new team **"CA-Office"**. You will create the public channels **"Support"** and **"Recruiting"**. Additionally, you will create the private channel **"Administration"** via Teams PowerShell.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. On the taskbar at the bottom of the page, right click the **Start** button and then select **Windows PowerShell**.
3. Run the following cmdlet to connect to Microsoft Teams in your tenant:

   ```
   Connect-MicrosoftTeams
   ```

4. A **Sign in** dialog box will open. Enter the **UPN** of **Joni Sherman's** O365 Credentials provided to you (for example, JoniS@<YourTenant>.onmicrosoft.com) and then select **Next**.
5. In the **Enter password** dialog box, enter the **password** of **Joni Sherman's** O365 Credentials provided to you and then select **Sign in**.
6. Type the following cmdlet to the PowerShell window to create the new team **CA-Office**:

   ```
   New-Team -Displayname "CA-Office" -MailNickName "CA-Office" -Visibility Public
   ```

7. To add the user **Alex Wilber** to the team type the following cmdlet (Replacing **<YourTenant>** with the name of the Microsoft 365 Tenant provided to you.):

   ```
   Get-Team -Displayname "CA-Office" | Add-TeamUser -User AlexW@<YourTenant>.onmicrosoft.com
   ```

8. To add the user **Allan Deyoung** to the team type the following cmdlet (Replacing **<YourTenant>** with the name of the Microsoft 365 Tenant provided to you.):

   ```
   Get-Team -Displayname "CA-Office" | Add-TeamUser -User AllanD@<YourTenant>.onmicrosoft.com
   ```

9. Create a channel **Support** in the **CA-Office** team by using the following cmdlet:

   ```
   Get-Team -Displayname "CA-Office" | New-TeamChannel -DisplayName "Support"
   ```

10. Create another channel **Recruiting** in the **CA-Office** team by using the following cmdlet:

    ```
    Get-Team -Displayname "CA-Office" | New-TeamChannel -DisplayName "Recruiting"
    ```

11. Create a private channel **Administration** in the **CA-Office** team by using the following cmdlet:

    ```
    Get-Team -Displayname "CA-Office" | New-TeamChannel -DisplayName "Administration" -MembershipType
    ```

12. Close the PowerShell window.
13. Open the Teams Desktop Client from the taskbar. On the left side pane with all teams Joni is a member of the new **CA-Office** team, where you can see a private channel below, named "Administration".
14. Close all browser windows and the Teams Desktop Client.

You have successfully created a team named **CA-Office** with the members Alex Wilber and Allan Deyoung. Joni Sherman is the only team owner. Note that you did not specify any owner in the PowerShell cmdlet and because it was run in context of Joni, she was added as owner automatically. Furthermore, you have created the public channels named **Support** and **Recruiting**, as well as the private channel named **Administration**.

17.4.1.3 Task 3 - 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Graph Explorer** at: https://developer.microsoft.com explorer
3. Select the **Sign in to Graph Explorer** button in the upper left of the page and sign in as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
4. If you access the Graph Explorer for the first time, you will see a **Permissions requested** page. Select **Accept**.
5. Select the **GET** button and select **POST** from the dropdown menu.
6. Do not change the **v1.0** from the box in the middle.
7. Enter the following to the text box next to the **Run query** button:
   - https://graph.microsoft.com/v1.0/teams
8. Select **Modify permissions** from the top pane.
9. Scroll to the right and select the **Consent** button for the permissions **Group.ReadWrite.All**.
10. Another **Permissions requested** page appears. Select **Accept**.
11. If you are redirected to the Microsoft Developers site, navigate back to the **Graph Explorer** at: https://developer.microsoft.com/graph/graph-explorer
12. Select the **Request body** tab and enter the following code:

```
{

"template@odata.bind":"https://graph.microsoft.com/v1.0/teamsTemplates('standard')",

"displayName": "Early Adopters",

"description": "The Early Adopters Workspace.",

"visibility": "Public"

}
```

13. Select **Run query** from the upper right of the page.
14. After a moment, you should see a green bar below the Request body window, with a checkmark and an **Accepted** message.
15. 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:

```
{

"template@odata.bind": "https://graph.microsoft.com/v1.0/teamsTemplates('standard')",

"visibility": "Public",

"displayName": "Tech Meetings",

"description": "Space for all employees participating in the champions program, who want exchange

"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&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,
"allowDeleteChannels": false,
"allowAddRemoveApps": true,
"allowCreateUpdateRemoveTabs": true,
"allowCreateUpdateRemoveConnectors": true
},
```

```
"guestSettings": {
"allowCreateUpdateChannels": true,
"allowDeleteChannels": false
},
"funSettings": {
"allowGiphy": true,
"giphyContentRating": "Moderate",
"allowStickersAndMemes": true,
"allowCustomMemes": true
},
"messagingSettings": {
"allowUserEditMessages": true,
"allowUserDeleteMessages": true,
"allowOwnerDeleteMessages": true,
"allowTeamMentions": true,
"allowChannelMentions": true
},
"discoverySettings": {
"showInTeamsSearchAndSuggestions": true
}
}
```

16. Select **Run query** from the upper right of the page.
17. After a moment, you should see a green bar with a checkmark and **Accepted** inside again.
18. Navigate to https://admin.teams.microsoft.com to access the Microsoft Teams web client.
19. 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.

17.4.1.4 Task 4 – 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Teams admin center**: https://admin.teams.microsof
3. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select **Teams** from the left-side pane and **Manage teams**.
5. Select the checkmark left from the **Sales** team and select **Archive** from the top pane.
6. Select the checkbox of **Make the SharePoint site read-only for team members** and select **Archive**.
7. The **Status** column should now have changed to **Archived**, written in orange color. Leave the browser open and proceed.
8. Connect to the **Client 2 VM** with the credentials that have been provided to you.
9. Open an Edge browser window and navigate to the **Microsoft Teams web client** page by entering the following URL in the address bar: **https://teams.microsoft.com/**.
10. On the **Pick an account** page, select the **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
11. Select **Use the webapp instead** to open the Teams web client.
12. On the left side, below the teams Megan is member or owner of, **Hidden teams** is now visible where team and channel names below are all written in italic. Select it to open the menu and select the **General** channel below the **Sales** team.
13. Try to write a new conversation by selecting **New conversation** from the bottom.
14. You will see a message **This team was archived, so you can't post more messages.** The archived status is also indicated by a small box icon, left from the three dots (…) menu, right from the team name.
15. Connect to the **Client 1 VM** again and use the credentials that have been provided to you.
16. Select the checkbox left from **Sales** again and select **Unarchive** from the top menu. The **Status** field should change to **Active** again.
17. Connect to the **Client 2 VM** again with the credentials that have been provided to you.
18. The text of the **Sales** team and the **General** channel changes back to normal after a moment, but the team is hidden. Select the three dots (…) right from the Sales team and select **Show**.
19. Leave the browser open and stay signed in.

You have successfully archived a team and reviewed the limited functionality of archived teams. This fulfils 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.

17.4.1.5 Task 5 - 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. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Teams web client** at **https://teams.microsoft.com**
3. On the **Pick an account** page, select the **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. 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.
5. In the **Delete "Sales" team**, select **I understand that everything will be deleted**. and select **Delete team**.
6. Leave the browser open and connect to **Client 1 VM** with the credentials that have been provided to you.
7. Open Microsoft Edge, maximize the browser, and navigate to the **Azure Portal** at: https://portal.azure.com.

8. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
9. In the **Enter password** dialog box, enter the password delivered by your training provider and select **Sign in**.
10. In the **Microsoft Azure portal**, below the **Azure services** section, select **More services**.
11. On the **All services** page, select **Identity** from the left side navigation pane and **Azure Active Directory** from the main window.
12. On the **Contoso | Overview** page, select **Groups** from the left side pane.
13. On the **Groups | All groups** page, select **Deleted groups** in the left side pane.
14. Now you can see all deleted groups, including the **Sales** group.
15. 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**.
16. Connect to **Client 2 VM** again with the credentials that have been provided to you.
17. Back on the **Teams web client**, press **F5** to refresh the page.
18. The **Sales** team appears in the list of teams again. Select the three dots (…) right from the team name and select **Manage team**.
19. 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 of this lab.

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

17.4.1.6 Task 6 - Manage team members with dynamic membership

Contoso 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Azure Portal** at: https://portal.azure.com.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
5. Select **Groups** from the left side pane.
6. In the **Groups | All groups** window, search and select **CA-Office** group.
7. In the **Group** settings, select **Properties** from the left-hand navigation pane.
8. In the **Membership type**, change it from **Assigned** to **Dynamic User**. Select **Add dynamic query** below **Dynamic user members**.
9. In the Dynamic membership rules window enter the following information to the fields:
   - Property: **accountEnabled**
   - Operator: **Equals**
   - Value: **true**
10. After this select **+add expression** and enter the following information to the fields:
    - Property: **usageLocation**
    - Operator: **Equals**
    - Value: **CA**
11. In the Dynamic membership rules window select **Save** in the top navigation pane.

12. In the **CA-Office| Properties** window select **Save** in the top navigation pane.
13. A warning message is displayed, that the membership will change according to the new dynamic membership rules. Select **Yes** to confirm the message.
14. Select **Overview** in the left-hand navigation pane of the **CA-Office** group window.
15. In the Overview window, locate **Membership 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.
16. 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.
17. 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.

17.4.2 Exercise 2: Manage sharing and access

In this exercise, you will test the guest access features in Office 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.

17.4.2.1 Task 1 - 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Sign in to the **Teams admin center** https://admin.teams.microsoft.com/ as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the **Microsoft Teams admin center** page, select the cogwheel from the lower left side pane and open the **Org-wide settings** menu.
4. Select **Guest access** from the list.
5. On the **Guest access** page, use the drop box right of **Allow guest access in Teams** and select **On**. Scroll down and select **Save**.
6. Close all browser windows.

You have now successfully activated guest access for Teams in your tenant.

17.4.2.2 Task 2 - Configure guest access in the Azure AD (optional)

In this task, you will configure the guest user access in the Microsoft Azure Portal. 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 need to have a personal Outlook.com account for this and the following tasks. If you don't have an account like this, open your web browser, go to **https://outlook.com** and create a new account.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Azure Portal**: https://portal.azure.com.
3. You should be still logged in as **MOD Administrator**. If not, on the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
5. Select **Users** from the left side pane.
6. In the **Users – All users** window, select **+ New guest user** from the top pane to create a new **Guest User**.

7. In the **New user** window select **Invite user** and enter the following information to the fields:
    - **Name**: your full name
    - **Email address**: your Outlook.com email address
    - **First name**: your First name
    - **Last name**: your last name
    - **Personal Message**: Hello Guest, Here is the link to access our Contoso test organization. Best regards, Contoso admin.
8. In the Groups and roles section, select **0 groups selected**. In the Groups window on the right side, select the **IT-Department** group, scroll down and return to the New user window by choosing **Select**.
9. To finish the invitation process, select **Invite** from the lower left side of the window.
10. You can now see a new user on the **Users − All users** page, note that the **User type** is set to **Guest**.
11. Open a **New InPrivate window** in your browser and go to the **Outlook Web Portal** page by entering the following URL in the address bar: **https://outlook.live.com/owa/**
12. In the top right navigation pane, select **Sign In**.
13. In the **Sign in** window, enter the **Email address** which you have created before.
14. In the **Enter password** dialog box, enter the password and select **Sign in**.
15. After signing in, open your **Inbox** and open the invitation Email with the topic **You're invited to the Contoso organization**.
16. When you select **Get Started** from the invitation Email, a new tab with a **Review permissions** message opens. Grant your consent to **Contoso** by selecting **Accept**.
17. Your personal outlook account has now been added to both your test tenant of Contoso Ltd. and to the "IT-Department" team.
18. Close the InPrivate window.

You have successfully changed the external collaboration settings, so guests can also invite new guests. Then you have added a personal outlook.com account as a guest to your tenant and as a member to the team "IT-Department".

17.4.2.3 Task 3 − Test external access with sensitivity labels (optional)

Even with enabled guest access sensitivity labels can deny guest access for specific teams. In this task you will try to add a guest user to an internal team. Enabling guest access for teams can take up to 24 hours. If you cannot find the guest user in step 4 you should test it again the next day.

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Open the Microsoft Teams Desktop Client, where you are signed in as **Megan Bowen**.
3. On the Teams overview select the three dots (**...**) right next to the Team "**Teams Rollout"** then select **Add member** from the dropdown list.
4. On the **Add members to Teams Rollout** page, enter the name of the guest user you just invited.
5. You will not be able to find the guest user, because guest users are restricted from this team.
6. Perform the steps 3 and 4 for the **Contoso** team, where you can find and add the guest user to the **Contoso** team.
7. Select **Close.**

Note: It can take up to 24 hours after enabling, till guest access is available in teams. If you cannot add guest users to any team, return to this task at a later point of this lab.

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.

17.4.2.4 Task 4 - Review access to a resource with access reviews

As a part of your system administrator role, you need to review access to resources in your tenant on a regular basis. You can do that by using access reviews in Microsoft Teams.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the browser, and navigate to the **Azure Portal**: https://portal.azure.com.
3. On the **Pick an account** page, select the **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
5. Select **Groups** from the left-hand navigation pane.
6. In the **Groups - All groups** window, select **Access reviews** in the left-hand navigation pane.
7. If you see the option **Onboard now** in the middle of the Page, select it and proceed to the next step. Otherwise, skip to step 13.
8. In the left-hand navigation pane select **Onboard**, to enable the **Access reviews** select **Onboard Now** at the bottom of the page.
9. After this you will return to the home of the **Azure Portal**. Select the **notification Bell** above the **navigation pane**. In the notification window you will see the message that the onboarding of the Access review was successful configured.
10. Close the notification window by selecting **X** in the right corner.
11. Select the search box on top of the window, type in **Azure Active Directory** and then select **Azure Active Directory**.
12. Select **Groups** from the left-hand navigation pane and on the **Groups - All groups** window, select **Access reviews** in the left-hand navigation pane again.
13. In the middle of the page select **+ New access review** and follow the steps below to create a new Access review.
    - On the **Review type** section of the **New access review** page, select the radio button beside **Select teams + Groups**
    - select **Select goroup(s)** and chose the Group: **IT-Department**
    - select the radio button beside **Guest users only**
    - select **Next:Reviews**
14. Under the **Reviews** section, follow the steps:
    - select **Group owner(s)** in the **Select reviewers** dropdown menu.
    - In the **Specify recurrence of review**, select **One time**, for **Duration (in days)** enter **7**, and use todays date for **Start date**
    - select **Next:Settings**
15. Under the **Settings** section, follow the steps:
    - set **Auto apply results to resource** to **enabled**, and leave others settings as default.
    - select **Next:Review+Create**
16. Under the **Review+Create** section, enter the following information to the fields:
    - Review name: **Guest access review**
    - Description: **Reviewing guest access**
    - Select **Create**.

    The system automatically creates an Email for the Access Reviewer.
17. In the browser window, select the circle with **MA** in the upper right corner, open the side pane and select **Sign out**.
18. Close your browser window and open it again by selecting the Edge browser icon from the taskbar.
19. In your browser, select the address bar and go to the **Outlook on the web** page by entering the following URL: **https://outlook.office365.com**

20. When you see the **Pick an account** window, select the **Joni Sherman account** to get to the Sign in window. If there is no **Joni Sherman account**, select **Use another account** to get to the Sign in window.
21. In the **Sign in** window, enter the UPN of **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and select **Next**.
22. In the **Enter password** dialog box, enter the password delivered by your training provider and select **Sign in**.
23. If a welcome screen appears, close it.
24. In the middle of the page, you will see an Email from **Microsoft Azure** with the topic **Action required: Review group access by <local date + 7 days in the future>**, then select this Email.
25. Select the **Start review** button in this Email.
26. An additional browser tab will open.
27. In the Access Review Window, you can see an overview with configured settings and the configured guest user with your personal outlook.com email address.
28. Select your outlook.com guest and then select **Details** to review the guest statistics.
29. Select **Deny** from the available options and select **Submit**.
30. In the overview, your outlook.com guest user has now **Denied** access.
31. Close all windows.

You have successfully created a new access review and blocked a guest user in your tenant. This is the end of lab 4. You can close all browser windows and proceed to the next lab.

17.5 END OF LAB

17.6 lab: title: 'Lab 04: Manage teams' module: 'Module 4: Deploy and manage teams'

18 Lab 04: Manage teams

19 Student lab manual

19.1 Lab Scenario

In the labs of this course, you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. 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 the second half of this lab, you will configure the guest access for your tenant and review access for both, internal and external users.

19.2 Objectives

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

- Create a Team from a Microsoft 365 Group
- Create a Team by using PowerShell
- Create a Team by using Microsoft Graph API
- Create a Team with dynamic membership
- Archive and unarchive Teams
- Delete and recover Teams
- Configure guest access in Azure and Teams
- Review Access to a resource

19.3 Lab Setup

- **Estimated Time:** 90 minutes.

19.4 Instructions

19.4.1 Exercise 1: Manage team resources

19.4.1.1 Task 1 - Create a team from an existing Microsoft 365 Group

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

1. Sign in to the **Teams Desktop client** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Create a new team from existing Microsoft 365 group with the following settings:
   - Name: **IT-Department**
   - Create from existing Microsoft 365 group: **IT-Department**
   - Owners: **Joni Sherman**
   - Members: **Lynne Robbins**, **Megan Bowen**, **Allan Deyoung** and **Alex Wilber**
3. Close the Teams Desktop client.

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.

19.4.1.2 Task 2 - Create a team by using PowerShell

In this task you will create via the Teams PowerShell a new team **"CA-Office"**. You will create the public channels **"Support"** and **"Recruiting"**. Additionally, you will create the private channel **"Administration"** via Teams PowerShell.

1. Open a **Windows PowerShell** window.
2. Connect to Teams in your tenant:

   ```
   Connect-MicrosoftTeams
   ```

3. Create a new team with the following settings, using the New-Team cmdlet:
   - Displayname: **CA-Office**
   - MailNickName: **CA-Office**
   - Visibility: **Public**
4. Use the GroupId from Get-Team and Add-TeamUser to add **Alex Wilbur** and **Allan Deyoung** as members to the team.
5. Use the GroupId from Get-Team and New-TeamChannel to create the regular channels **"Support"** and **"Recruiting"**.
6. Use the GroupId from Get-Team and New-TeamChannel to create the private channel **"Administration"**.
7. Close the PowerShell window.

You have successfully created a team named **CA-Office** with the members Alex Wilber and Allan Deyoung. Joni Sherman is the only team owner. Note that you did not specify any owner in the PowerShell cmdlet and because it was run in context of Joni, she was added as owner automatically. Furthermore, you have created the public channels named **Support** and **Recruiting**, as well as the private channel named **Administration**.

19.4.1.3 Task 3 - 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. Sign in to the **Graph Explorer** (https://developer.microsoft.com/graph/graph-explorer) using **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).
2. If you see a **Permissions requested** page, select **Accept**.
3. Enter the following to the text box next to the **Run query** button:
   - https://graph.microsoft.com/v1.0/teams
4. Select **Modify permissions** from the top pane.
5. Scroll to the right and select the **Consent** button for the permissions **Group.ReadWrite.All**. And accept the permissions.
6. Select the **Request body** tab and run the following code to create a new team:

```
{

 "template@odata.bind":"https://graph.microsoft.com/v1.0/teamsTemplates('standard')",

 "displayName": "Early Adopters",

 "description": "The Early Adopters Workspace.",

 "visibility": "Public"

 }
```

7. Run a second command in the **Request body** tab and create another team:

```
{

 "template@odata.bind": "https://graph.microsoft.com/v1.0/teamsTemplates('standard')",

 "visibility": "Public",

 "displayName": "Tech Meetings",

 "description": "Space for all employees participating in the champions program, who want exchange

 "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&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,
"allowDeleteChannels": false,
"allowAddRemoveApps": true,
"allowCreateUpdateRemoveTabs": true,
"allowCreateUpdateRemoveConnectors": true
},
"guestSettings": {
"allowCreateUpdateChannels": true,
"allowDeleteChannels": false
},
"funSettings": {
"allowGiphy": true,
"giphyContentRating": "Moderate",
"allowStickersAndMemes": true,
"allowCustomMemes": true
},
"messagingSettings": {
"allowUserEditMessages": true,
"allowUserDeleteMessages": true,
"allowOwnerDeleteMessages": true,
```

```
"allowTeamMentions": true,
"allowChannelMentions": true
},
"discoverySettings": {
"showInTeamsSearchAndSuggestions": true
}
}
```

8. Navigate to the **Teams admin center** (https://admin.teams.microsoft.com/) 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.

19.4.1.4 Task 4 – 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. Sign in to the **Teams admin center** **https://admin.teams.microsoft.com** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. In **Teams**, under **Manage teams**, select the **Sales** team and select **Archive**.
3. Select the checkbox of **Make the SharePoint site read-only for team members** and select **Archive**.
4. Inspect the **Status** of the team.
5. Connect to the **Client 2 VM** with the credentials that have been provided to you.
6. Sign in to **Microsoft Teams web client** (https://teams.microsoft.com) as user **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
7. In the **Microsoft Teams web client**, under **Hidden teams**, select the **Sales** team and start a new conversation in the **General** channel.
8. You will see a message **This team was archived, so you can't post more messages.** The archived status is also indicated by a small box sign, left from the three dots (…) menu, right from the team name.
9. Connect to the **Client 1 VM** again and use the credentials that have been provided to you.
10. In **Teams**, under **Manage teams**, select the **Sales** team and select **Unarchive**.
11. Connect to the **Client 2 VM** again with the credentials that have been provided to you.
12. Inspect the changes to the **Sales** team.

You have successfully archived a team and reviewed the limited functionality of archived teams. This fulfils 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, for making it fully operational again.

19.4.1.5 Task 5 - 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. Sign in to the **Teams web client** at **https://teams.microsoft.com** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
2. Delete the **Sales** team.

3. Sign in to the **Azure Portal** https://portal.azure.com/ using **MOD Administrator** (admin@<YourTenant>.onmicros
4. Navigate to **Azure Active Directory** and **Deleted groups**.
5. Restore the **Sales** team.
6. Check the **Teams web client** for the recovered group.

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 of this lab again.

You have successfully deleted and restored a via the Teams Desktop client and Azure Admin Portal.

19.4.1.6 Task 6 - Manage team members with dynamic membership

Contoso 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. Sign in to the **Azure Portal** https://portal.azure.com/ using **MOD Administrator** (admin@<YourTenant>.onmicros
2. Navigate to **Azure Active Directory** and **Groups**.
3. Switch **CA-Office** to a group with Dynamic membership, using the following expression:
   - Property: **accountEnabled**
   - Operator: **Equals**
   - Value: **true**
4. Add a second expression:
   - Property: **usageLocation**
   - Operator: **Equals**
   - Value: **CA**
5. Check the **Membership processing status** for members with the correct usage location.
6. Close the Azure Portal.

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.

19.4.2 Exercise 2: Manage sharing and access

In this exercise, you will test the guest access features in Office 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.

19.4.2.1 Task 1 - Configure guest access in Teams

In this task, you will configure the guest user access for Microsoft Teams in your tenant.

1. Sign in to the **Teams admin center** https://admin.teams.microsoft.com/ as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Change the Org-wide settings and allow **Allow guest access in Teams**.
3. Close the Teams admin center.

You have now successfully activated guest user access in Teams for your tenant.

19.4.2.2 Task 2 - Configure guest access in the Azure AD (optional)

In this task, you will configure the guest user access in the Microsoft Azure Portal. 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 need to have a personal outlook.com account for this and the following tasks. If you don't have an account like this, open your web browser, go to https://outlook.com and create a new account.

1. Sign in to the **Azure Portal** https://portal.azure.com/ using **MOD Administrator** (admin@<YourTenant>.onmicros

2. Navigate to **Azure Active Directory** and **Users**.
3. Create a new guest user with the following settings:
   - **Name:** your full name
   - **Email address:** your Outlook.com email address
   - **First name:** your First name
   - **Last name:** your last name
   - **Personal Message:** Hello Guest, here is the link to access to our Contoso test organization. Best regards, Contoso admin.
   - **Groups**: IT-Department
4. Sign in to the **Outlook Web Portal** (https://outlook.live.com/owa/) using your personal account.
5. Grant consent and explore the guest access.

You have successfully changed the external collaboration settings, so guests can also invite new guests. Then you have added a personal outlook.com account as a guest to your tenant and as a member to the team "IT-Department".

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

Even with enabled guest access sensitivity labels can deny guest access for specific teams. In this task you will try to add a guest user to an internal team. Enabling guest access for teams can take up to 24 hours. If you cannot find the guest user in step 4, you should test it again the next day.

1. Sign in to the **Teams Desktop client** using **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft.com).
2. Add the guest user you just invited to the **Teams Rollout** team. You will not be able to find the guest user, because guest users are restricted from this team.
3. Add the guest user to the **Contoso** team and observe the differences.

Note: After enabling, it can take up to 24 hours before guest access is available in teams. If you cannot add guest users to any team, return to this task at a later point of this lab.

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.

19.4.2.4 Task 4 - Review access to a resource with access reviews

As a part of your system administrator role, you need to review access to resources in your tenant on a regular basis. You can do that by using access reviews in Microsoft Teams.

1. Sign in to the **Azure Portal** https://portal.azure.com/ using **MOD Administrator** (admin@<YourTenant>.onmicros
2. Navigate to **Azure Active Directory** and **Groups**.
3. Onboard to **Access reviews** and create a new access review with the following settings:
   - Review name: **Guest access review**
   - Description: **Reviewing guest access**
   - StartDate: **your current date**
   - Frequency: **One time**
   - EndDate: **your current date + 7 days into the future**
   - Scope: **Guest users only**
   - Group: **IT-Department**
   - Reviewers: **Group owners**
4. Navigate to **Outlook on the web** https://outlook.office365.com using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
5. Review the access reviews mail and deny access for the guest user in the **IT-Department** team.

6. Close the Outlook on the web window.

You have successfully created a new access review and blocked a guest user in your tenant. This is the end of lab 4. You can close all browser windows and proceed to the next lab.

19.5 END OF LAB

19.6 lab: title: 'Lab 05: Modify collaboration settings for Teams' type: 'Answer Key' module: 'Module 5: Manage collaboration in Microsoft Teams'

20 Lab 05: Modify collaboration settings for Teams

21 Student lab answer key

21.1 Lab Scenario

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 setup policies, Apps, bots & connectors in Microsoft Teams or publish a custom app in Microsoft Teams.

21.2 Objectives

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

- Create a messaging policy
- Manage private channels
- Disable third party storage providers
- Create a Power Apps app
- Manage Policy packages
- Upload a tenant wide custom line of business app
- Edit and test default org-wide app policy
- Edit and test default app permission policy

21.3 Lab Setup

- **Estimated Time:** 90 minutes.

21.4 Instructions

21.4.1 Exercise 1: 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.

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

In the past, some users of Contoso have used a lot of stickers, gif animations and similar pictures in their conversations, even with externals using other chat solutions. The new corporate guideline shall prohibit the use of graphic elements in corporate communication via Teams, because users shall not use them in conversations with external customers and clients. As a Teams service administrator, you must create a new message policy that prohibits its use and apply it to several users of your pilot project.

Note: After creating a messaging policy, it can take up to 24 hours for the settings to be applied to the users.

1. Connect to the Client 1 VM with the credentials that have been provided to you.
2. Open **Microsoft Edge**, maximize the window and navigate to the **Teams admin center** at **https://admin.teams.microsoft.com/**.
3. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.

4. In the left-hand navigation pane, select the **Messaging policies**, then click on the **+ Add** at the right side of the page, to create a new messaging policy.
5. In the **New messaging policy** dialog enter the following information to the fields and set the following configuration:
   - **Name**: Regular users without fun stuff
   - **Description**: Policy to disable giphys, stickers, and memes in conversations
   - **Use Giphys in conversations**: off
   - **Use Memes in conversations**: off
   - **Use Stickers in conversations**: off
6. Leave the rest of the settings as default. Select **Save**.
7. In the Messaging policies overview, select the checkmark left to **Regular users without fun stuff**. Then select **Manage users** in the top navigation pane. If you cannot see **Manage users**, you may need to select the three dots first.
8. Type in **Lynne Robbins** and select **Add**, and then select **Apply**.
9. Stay in the Teams admin center and continue with the next task.

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

21.4.1.2 Task 2 - Manage private channels in a team

As Teams administrator of Contoso, you will create a private channel "confidential" in the sales team that only allows some people to be able to access the information.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in as **Joni Sherman** in the **Microsoft Teams Admin center**.
3. In the left-hand navigation pane, select **Teams** to open the menu and **Manage teams** below.
4. Select the **Sales** team in the **Manage teams** overview window.
5. Select the **Channels** tab in the middle of the page. Select **+ Add** in the navigation pane below to get into the **Add channel** window.
6. In the **Add channel** window enter the following information:
   - **Name:** Confidential sales
   - **Description:** Confidential private sales channel
   - **Type:** Private
7. Enter to the field **Channel owner** the user **Lynne Robbins** and select her as owner.
8. Select **Apply** in the **Add channel** window.
9. Connect to the **Client 2 VM** with the credentials that have been provided to you.
10. Open the Edge browser with the icon from the taskbar.
11. In your browser, select the address bar and go to the **Teams Web Client** page by entering the following URL: **https://teams.microsoft.com**
12. On the **Pick an account** page, select the **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
13. On the Microsoft Teams landing page click **Use the web app instead**.
14. On the team overview in the Teams web client, 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.

21.4.2 Exercise 2: Manage app settings

21.4.2.1 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.

Note: After disabling the third-party storage provider, it can take up to 24 hours for the settings to be applied to the teams.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in as **Joni Sherman** in the **Microsoft Teams Admin center**.
3. On the left-side navigation pane, select the **Org-wide settings** to open the menu, then select **Teams settings** below.
4. In the Teams settings overview go to the **Files** section. Configure the following file sharing and cloud file storage options.
   - **Citrix files:** Off
   - **DropBox:** Off
   - **Box:** On
   - **Google Drive:** Off
   - **Egnyte:** Off
5. After this scroll down and select **Save**.

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

21.4.2.2 Task 2 - Edit default org-wide app policy

In the pilot project, the company decided that Microsoft Planner is the default app for all (existing) teams. To do this, edit the default org-wide app policy. This task may take some time to propagate throughout the tenant.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in as **Joni Sherman** in the **Microsoft Teams Admin center**.
3. In the left-hand navigation pane, select the **Teams apps** to open the menu, then select **Setup policies**.
4. In the **App setup policies** window select **Global (Org-wide default)** name to open the org-wide app policy.
5. In the **Pinned apps** section select **+ Add apps** to open the **Add pinned apps** menu at the right side.
6. Select **Global** and type in the name **Planner**, mouseover the presented name and select **Add**. After this, select **Add** to return previous window.
7. Make sure that **Planner** is now listed in the **Pinned apps** section and select **Save**.
8. In the **App setup policies** window select **Global (Org-wide default)** and make sure there is a selected checkmark in the front of the name.
9. Then select **Manage users** in the top navigation pane to open the **Mange users** dialog. Enter the name of **Lynne Robbins** and mouseover the presented name and select **Add**. Then select **Apply**.
10. Connect to the **Client 2 VM** with the credentials that have been provided to you.
11. Open the Edge browser, select the address bar and go to the **Teams Web Client** page by entering the following URL: **https://teams.microsoft.com**
12. On the **Pick an account** window, select LynneR@<YourTenant>.onmicrosoft.com and sign in.
13. On the Microsoft Teams landing page click **Use the web app instead**.
14. In the left-hand navigation pane, the **Planner** app should be displayed by default below the Files **menu**.

21.4.2.3 Task 3 - Edit default app permission policy

In this task you will edit the default app permission policy and block the Google Analytics app for all tenants

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in as **Joni Sherman** in the **Microsoft Teams Admin center**.
3. In the left-hand navigation pane, select the **Teams apps** to open the menu, then select **Permission policies**.
4. In the **App permission policies** window select **+ Add** to create a new policy.
5. After this the policy creation dialog appears, type in the policy name **Block Google Analytics** and expand the menu in the **Third-party app** section, and select **Block specific apps and allow all others**.
6. Select **Block apps** below the Notification **Add apps that you want to block** to open the right-side menu.
7. In the Add third party apps dialog, type in **Google Analytics**, mouseover the presented name and select **Add**. Repeat the same step for **Google Analytics Insights**. After this select **Block** to return to the **App permission policies** window. Select **Save**.
8. In the App permission policies overview, select the checkmark left to **Block Google Analytics**. Then select **Manage users** in the top navigation pane.
9. Type in **Lynne Robbins** and select **Add** by mouseover the presented name, then click **Apply**.

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

21.4.2.4 Task 4 – 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. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. You are still signed in as **Joni Sherman** in the **Microsoft Teams Admin center**.
3. In the left-hand navigation pane, select **Policy packages** to display existing policy packages.
4. Review the existing policy packages. Afterwards select **Firstline worker** to edit the policy package.
5. From the list of assigned policies, select **Firstline_Worker** right from **Messaging policy**.
6. Select **Edit** from the upper right corner to change the policy settings.
7. Select the switch right from **Send urgent messages using priority notifications** to **On** and select **Save**.
8. Back on the list of assigned policies, select **Firstline_Worker** right from **Calling policy**.
9. Select the switch right from **Prevent toll bypass and send calls through the PSTN** and **Busy on busy is available when in a call** to **On** and select **Save**.
10. Back on the list of assigned policies again, select **Back** to go to the Policy packages overview.
11. The checkmark left from the **Firstline worker** policy package is still active. Select **Manage users** from the top pane to open the **Manage users** right-side pane.
12. Type "Allan" into the search bar, select **Add** right from **Allan Deyoung** and **Apply**.
13. Select **Users** from the left-side pane.
14. In the line of Allan Deyoung, select **View policies**.
15. Below Assigned policies you can now see the different **Firstline_Worker** policies and below **Policy package** the **Firstline worker** package.

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.

21.4.2.5 Task 5 - Add a custom line of business app

In this task, you will add a custom line of business app required for your company Contoso Ltd. for all users of your tenant. You find sample LOB app at: https://github.com/OfficeDev/msteams-sample-line-of-business-apps-csharp.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Select the **Edge Browser** icon from the taskbar. In your browser go to the following link and download the custom line of business app as zip package:
   - Go to the following link: **Notification Bot**.
   - Select **Download** and **Save**, to download the file to the **Downloads** folder.
3. Navigate to the **Microsoft Teams web client** page by entering the following URL in the address bar: **https://teams.microsoft.com/**
4. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
5. On the teams landing page, select **Use the web app instead**.
6. Select **Apps** from the side pane.
7. Scroll down the list of **Apps**, select **Upload a custom app** and **Upload for Contoso**.
8. A file select window appears. Navigate to **Downloads** and select **Notification App.zip**.
9. Go back to **Apps** from the side pane.
10. Select **Built for Contoso**.
11. Note the **NotificationBot** app.
12. Select **Joni Shermans** picture in the upper right corner and select **Sign out**. Close the Edge browser.
13. Connect to the **Client 2 VM** with the credentials that have been provided to you.
14. Select the **Edge Browser** icon from the taskbar. In your browser go to the **Microsoft Teams web client** page by entering the following URL in the address bar: **https://teams.microsoft.com/**
15. On the **Pick an account** page, select the **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
16. On the teams landing page, select **Use the web app instead**.
17. Go back to **Apps** from the side pane.
18. Scroll down and select **Built for Contoso**.
19. Select **NotificationBot** and review the details.
20. Select **Add for me**, to test the custom app.
21. On the **Welcome to Notification Bot** conversation, select the dropdown menu and select **Weather**, and then select **Show Notification**.
22. The weather forecast for your location is being displayed.
23. Close all browser windows.

You have successfully added a custom app to your tenant with the account of Joni Sherman, who is a Teams admin in your tenant. Afterwards, you have successfully tested the app availability with a regular user.

21.4.2.6 Task 6 - Add a custom app from Microsoft Power Apps

In this task, you will need to evaluate the integration of Power Apps into Teams by creating a new app from a template and integrate it into the IT-Department team. You will choose the Out of Office template and provide a fast option for IT-Department members to activate the Out of Office function for their mailbox.

1. Connect to the **Client 1 VM** with the credentials that have been provided to you.
2. Open Microsoft Edge, maximize the window and navigate to **https://make.powerapps.com** to access the **Power Apps** dashboard.

3. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. Select **+ Create** from the left-side menu and scroll down to **Start from template**.
5. Select the **Out of Office** tile with **Canvas app** text below to open the creation dialog.
6. Below **App name** enter the following: **MyOofApp**.
7. Select **Phone** below Format and **Create**.
8. If you see a **Choose your country/region to get started** message, leave the default selection and select **Get started**.
9. A new tab is opened. When the **Almost there...** frame appears, select **Allow**.
10. When a **Welcome to Power Apps Studio** frame appears, select **Don't show me this again** and **Skip**.
11. When a **Preview features entering final validation** frame appears, select **Open app** to continue.
12. When the app editor has loaded, select the paint bucket from the top pane and select your favorite color to change the background of the WelcomeScreen page of your app.
13. Review the other app pages from the left-side pane, below **Tree view** but do not do any more changes.
14. After reviewing the settings, select the play button (rectangle) from the upper right corner to test your app.
15. Select **Create new**, enter the following values, and select **Next**:
    - **Set response start time** the next day from 08:00 am.
    - **Set response end time** the next day until 06:00 pm.
    - **Title (optional)** I'm out of office.
16. On the **Select response type** page, select **Business** and **Next**.
17. On the **Select email access** page, select **Intermittent** and **Next**.
18. On the **Select alternate contacts** page, select down arrow right from **Find contacts**, select IT-Department and select **Next**.
19. Review the sample text, but do not select **Submit**. Select the **X** from the upper right corner instead.
20. When you see a **Did you know?** frame, select **Don't show me this again** and **Ok**.
21. Select **File** from the upper left in the top pane and **Save as**.
22. Change the default app name to **MyOofApp** and select **Save**.
23. When you see the **All changes are saved.** message, you have successfully created a new Power App. Select **Share** to manage access to your app.
24. On the **Share MyOofApp** page enter **Everyone** to the search box and select the **Everyone in Contoso**.
25. Leave the default settings and select **Share** from the lower right of the page.
26. Close the Edge browser and switch to Client 2 VM.
27. Connect to the **Client 2 VM** with the credentials that have been provided to you.
28. Select the **Edge Browser** icon from the taskbar. In your browser go to the **Microsoft Teams web client** page by entering the following URL in the address bar: **https://teams.microsoft.com/**
29. On the Pick an account page, select LynneR@<YourTenant>.onmicrosoft.com and sign in with the credentials provided.
30. On the teams landing page, select **Use the web app instead**.
31. Select the **General** channel below **IT-Department**.
32. Select the + symbol from the top pane, enter **Power** to the search box and select **Power Apps**.
33. Select **Add** to integrate Power Apps to your IT-Department team.
34. On the next **Power Apps** page, select the **MyOofApp** and select **Save**.

35. You have successfully pinned the **MyOofApp** to the **General** channel of your **IT-Department** team.

In this task, you have successfully created a Power App and integrated it into a Teams channel. All members of the IT-Department team can now use the app in the tab to plan and create an Out of Office (Oof) message for their mailboxes.

21.4.3 Exercise 3: 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.

21.4.3.1 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 affected user (Lynne Robbins) vs regular user(Joni Sherman).

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. Select the **Edge Browser** icon from the taskbar. In your browser, go to the **Microsoft Teams web client** page by entering the following URL in the address bar: **https://teams.microsoft.com/**
3. On the **Pick an account** page, select the **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. On the Microsoft Teams landing page click **Use the web app instead**.
5. Skip a potential welcome dialog by selecting on **x** in the right corner.
6. In the left-hand navigation pane, select **Chat**, then select the **Contacts** in the dropdown menu.
7. If there is no contact for **Joni Sherman**, then select **...** and select **Add a contact to this group**. Type in the name **Joni Sherman** and select her by mouseover the presented name. After this select **Add** to return to the **Contacts tab**.
8. In the **Contacts** tab, select **Joni Sherman**. Note that if the **giphy**, **memes** and **stickers** icons are missing below the conversation-bar, the **messaging policy** has taken effect.
9. In the left-hand navigation pane, select **Teams**.
10. Select the **Confidential sales** channel of the **Sales** team and add a comment to confirm that you have access to the private channel.

21.4.3.2 Task 2 – Test the app permission policy and storage providers

In this task, you will test the **app permission policies** configured in exercise 2 and compare the differences between affected user (Lynne Robbins) vs regular user (Joni Sherman).

1. Connect to the **Client 2 VM** with the credentials that have been provided to you.
2. You are still in the **Teams web client** and signed in as **Lynne Robbins**.
3. In the left-hand navigation select **Teams** and select the **IT-Department** channel **General**. Mouseover the presented name **General**, select **...** and then select **Connectors**.
4. In the **Connectors for "General"** window, enter **Google Analytics** into the search field.
5. If you can't find **Google Analytics** as a search result and can't add the app to the channel, the **app permission policy** has worked as desired.
6. In the left-hand navigation pane, select **Teams**, then select the **IT-Department** team. Select the **files** Tab on the middle of the Teams web client. Then select **+ Add cloud storage** in the navigation pane below.
7. If 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.

21.5 END OF LAB

21.6 lab: title: 'Lab 05: Modify collaboration settings for Teams' module: 'Module 5: Manage collaboration in Microsoft Teams'

22 Lab 05: Modify collaboration settings for Teams

23 Student lab manual

23.1 Lab Scenario

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 setup policies, Apps, bots & connectors in Microsoft Teams or publish a custom app in Microsoft Teams.

23.2 Objectives

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

- Create a messaging policy
- Manage private channels
- Disable third party storage providers
- Create a Power Apps app
- Manage Policy packages
- Upload a tenant wide custom line of business app
- Edit and test default org-wide app policy
- Edit and test default app permission policy

23.3 Lab Setup

- **Estimated Time:** 90 minutes.

23.4 Instructions

23.4.1 Exercise 1: 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.

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

In the past, some users of Contoso have used a lot of stickers, gif animations, and similar pictures in their conversations, even with externals using other chat solutions. The new corporate guideline shall prohibit the use of graphic elements in corporate communication via Teams, because users shall not use them in conversations with external customers and clients. As a Teams service administrator, you must create a new message policy that prohibits its use and apply it to several users of your pilot project.

Note: After creating a messaging policy, it can take up to 24 hours for the settings to be applied to the users.

1. Sign in to the **Teams admin center** **https://admin.teams.microsoft.com** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Create a new **New messaging policy** with the following settings:
    - **Name:** Regular users without fun stuff
    - **Description:** Policy to disable giphys, stickers, and memes in conversations
    - **Use Giphys in conversations:** off
    - **Use Memes in conversations:** off
    - **Use Stickers in conversations:** off

3. Assign the new messaging policy to **Lynne Robbins**.
4. Leave the Teams admin center open.

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

23.4.1.2 Task 2 - Manage private channels in a team

As Teams administrator of Contoso, you will create a private channel "confidential" in the sales team that only allows some people to be able to access the information.

1. Sign in to the Teams admin center **https://admin.teams.microsoft.com/** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Create a new channel for the **Sales** team, using the following settings:
   - **Name:** Confidential sales
   - **Description:** Confidential private sales channel
   - **Type:** Private
   - **Owner:** Lynne Robbins
3. Sign in to the Teams web client **https://teams.microsoft.com/** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
4. Check the existence of the new channel.
5. Close the Teams web client.

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.

23.4.2 Exercise 2: Manage app settings

23.4.2.1 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.

Note: After disabling the third-party storage provider, it can take up to 24 hours for the settings to be applied to the teams.

1. Sign in to the Teams admin center **https://admin.teams.microsoft.com/** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Change the **Teams settings** to the following values:
   - **Citrix files:** Off
   - **DropBox:** Off
   - **Box:** On
   - **Google Drive:** Off
   - **Egnyte:** Off
3. Leave the Teams admin center open.

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

23.4.2.2 Task 2 - Edit default org-wide app policy

In the pilot project, the company decided that Microsoft Planner is the default app for all (existing) teams. To do this, edit the default org-wide app policy

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

2. Edit the **App setup policies** with the name **Global (Org-wide default)** to the following settings:
    - **Pinned apps:** Planner
3. Make sure **Lynne Robbins** has the **App setup policies** with the name **Global (Org-wide default)** configured.
4. Sign in to the Teams web client **https://teams.microsoft.com/** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
5. Check, that **Planner** is present as new pinned app.
6. Close the Teams web client.

23.4.2.3 Task 3 - Edit default app permission policy

In this task you will edit the default app permission policy and block the Google Analytics app for all tenants

1. Sign in to the Teams admin center **https://admin.teams.microsoft.com/** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Create a new **App permission policies** with the following settings:
    - Name: **Block Google Analytics**
    - **Block specific apps and allow all others**
    - Block third party apps: **Google Analytics** and **Google Analytics Insights**
3. Assign the **App permission policy** to **Lynne Robbins**.
4. Close the Teams admin center.

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

23.4.2.4 Task 4 – 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. Sign in to the Teams admin center **https://admin.teams.microsoft.com/** using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Select **Policy packages** and review the existing policy packages.
3. **Edit** the **Messaging policy** of the **Firstline_Worker** package with the following setting:
    - **Send urgent messages using priority notifications**: On
4. **Edit** the **Calling policy** of the **Firstline_Worker** package with the following settings:
    - **Prevent toll bypass and send calls through the PSTN**: On
    - **Busy on busy is available when in a call**: On
5. Add **Allan Deyoung** to the policy package.
6. Select **Users** and review the policies for **Allan Dyoung**. You should see **Firstline worker** package and the **Firstline_Worker** policies.

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.

23.4.2.5 Task 5 - Add a custom line of business app

In this task, you will add a custom line of business app required for your company Contoso Ltd. for all users of your tenant. You find sample LOB app at: **https://github.com/OfficeDev/msteams-sample-line-of-business-apps-csharp**.

1. Download the custom app from the following links: **Notification Bot**.

2. Sign in to the Teams web client **https://teams.microsoft.com** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
3. Upload the custom app in **Apps**.
4. Interrogate with the new app to receive a weather forecast.
5. Close the Teams web client.

You have successfully added a custom app to your tenant with the account of Joni Sherman, who is a Teams admin in your tenant. Afterwards, you have successfully tested the app availability with a regular user.

23.4.2.6 Task 6 - Add a custom app from Microsoft Power Apps

In this task, you will need to evaluate the integration of Power Apps into Teams by creating a new app from a template and integrate it into the IT-Department team. You will choose the Out of Office template and provide a fast option for IT-Department members to activate the Out of Office function for their mailbox.

1. Sign in to the **Power Apps** dashboard (**https://make.powerapps.com/**) using **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. Open the app editor and create a new **Power App** called MyOofApp from the **Out of Office** template.
3. Test the app and explore the options the app provides under **create new**.
4. Share the app with **Everyone in Contoso**.
5. Sign in to the Teams web client **https://teams.microsoft.com** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
6. Using the **Microsoft Teams Desktop Client** pin your new **Power App** to the **General** channel of the **IT-Department** team.

In this task, you have successfully created a Power App and integrated it into a Teams channel. All members of the IT-Department team can now use the app in the tab to plan and create an Out of Office (Oof) message for their mailboxes.

23.4.3 Exercise 3: 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.

23.4.3.1 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 affected user (Lynne Robbins) vs regular user(Joni Sherman).

1. Sign in to the Teams web client **https://teams.microsoft.com** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
2. Open a chat with **Joni Sherman** and check, if the **messaging policy** works as expected.
3. Write a message to the **Confidential Sales** channel conversation window.

23.4.3.2 Task 2 – Test the app permission policy and storage providers

In this task, you will test the **app permission policies** configured in exercise 2 and compare the difference between affected user (Lynne Robbins) vs regular user (Joni Sherman).

1. Sign in to the Teams web client **https://teams.microsoft.com** using **Lynne Robbins** (LynneR@<YourTenant>.onmicrosoft.com).
2. Try to add an additional **Google Analytics** connector to the **IT-Department** team. If this does not work, the **app permission policy** works as desired.
3. Try to add non-SharePoint storage providers to the **IT-Department** team. If you only see Box as an alternative, the configured **Teams settings** works as expected.
4. Close the Teams web client.

23.5 END OF LAB

23.6 lab: title: 'Lab 06: Manage communication in Microsoft Teams' type: 'Answer Key' module: 'Module 6: Manage communication in Microsoft Teams'

24 Lab 06: - Manage communication in Microsoft Teams

25 Student lab answer key

25.1 Lab Scenario

In the labs of this course you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. and her pilot team that shall evaluate the capabilities of Microsoft Teams in a testing environment. According to Contoso business requirements, Microsoft Teams will be used as an organization's solution for conferencing and telephony. Therefore, Teams admins need to configure conferencing functionalities, such as meetings and live event features that will provide best user experience during collaboration and communication. Furthermore, Teams admins will need to replace Contoso legacy PBX solution and configure voice features that will provide users with Teams calling capabilities.

25.2 Objectives

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

- Manage meeting policies
- Configure meeting settings
- Create live event policies
- Create a live event
- Configure emergency addresses
- Create calling policies
- Configure resource accounts and calling queues
- Create resource accounts and auto attendants
- Test configured meeting policies
- Test configured meeting settings
- Set up a Calling Plan
- Order and Assign phone numbers

25.3 Lab Setup

- **Estimated Time:** 90 minutes.

25.4 Instructions

25.4.1 Exercise 1: Manage Live event and meetings experiences

Contoso organization has deployed Microsoft 365 and is testing pilot projects on collaboration and communication scenarios to meet business requirements. First, Teams admins need to configure meeting policies and schedule initial meetings. Then, business managers want to test the Live meetings option in Microsoft Teams in order to broadcast audio and video to large audiences.

25.4.1.1 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 fulfil 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.

2. Open **Microsoft Edge**, maximize the window and navigate to the **Teams admin center** at **https://admin.teams.microsoft.com/**.
3. On the **Pick an account** page, select the **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.
4. If a **Stay signed in?** dialog box is displayed, select the **Don't show this again** checkbox and **Yes**.
5. In the **Teams admin center,** on the left navigation pane, select **Meetings,** and then choose **Meeting policies**.
6. Select the **Global (Org-wide default)** policy to change the settings for all users.
7. On the **Meetings policies\Global** page, review the available settings, and under **Audio & Video** section, use the slider to turn **Off** the **Allow cloud recording** setting. 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.

25.4.1.2 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. Connect to the **Client 2 VM** and sign in with the Credentials that have been provided to you.
2. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
3. Select **Calendar** from the left navigation pane and **Meet Now** from the upper right corner to start a meeting.
4. On the Microsoft Teams page, leave the default settings and select **Join now** button.
5. On the Microsoft Team page, hover the mouse over the meeting page, and select the three dots (…) for **More actions**.
6. Note that **Start recording** option is visible but is dimmed, not available to be selected.

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

Contoso Ltd. 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
3. On the left navigation pane, select **Meetings,** and then choose **Meetings settings**.
4. On the **Meetings settings** page, below participants, use the slider to turn **Off** the option **Anonymous users can join a meeting**.
5. 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.

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

Contoso 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 Contoso Ltd. business requirements, you will need to restrict the recording options for participants of meetings and only allow recording options to management users. Only the organizer of a live event should be able to record his own meetings.

1. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.

2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
3. On the left navigation pane, select **Meetings** and then select **Live event policies**.
4. Select **+ Add** from the top pane, to create a new **Live event policy** with individual settings for assigned users.
5. On **Live event policies\Add** page, enter the following information:
   - Add live events policy: **Management Live Events**
   - Description: **Recording Restriction for live events organized by managers**
   - Allow scheduling: **On**
   - Allow transcription for attendees: **Off**
   - Who can join scheduled live events: **Everyone in the organization**
   - Who can record an event: **Organizer can record**
6. Select **Save**.
7. Back on the **Live events policies** page, use the checkbox left of **Management Live Events** and select **Manage users** from the top pane to assign the new policy to users.
8. In the right-side pane, type into the search field **Megan Bowen** and Add right from her name.
9. 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.

25.4.1.5 Task 5 – Create a new live event

Contoso Ltd. Wants to broadcast video and meeting content to large online audiences using Teams live events. As a Teams admin, you need to demonstrate the functionality of live meetings to Management.

1. Connect to the **Client 2 VM** and sign in with the Credentials that have been provided to you.
2. Open the Teams Desktop client from the taskbar, where you are still signed in as **Megan Bowen**.
3. On the left navigation pane select **Calendar**.
4. In the top right select the arrow next to **new meeting** and select **live event** in the dropdown menu.
5. Create a new **live event**:
   - Title: Management Showcase
   - Start/End: Select a time close to your current time
6. Select **Next**.
7. Under **Live event permissions** select **Org-Wide**.
8. Under **How will you produce your live event?** Select **Teams**.
9. Select **Schedule**.
10. On the next page select **Get attendee link** and send it in a chat message to Joni Sherman.
11. On the left navigation pane select **Calendar**.
12. Select the **live event** named **Management Showcase**.
13. In the information window select **Join** to join the meeting.
14. In the meeting preparation window select **Join now**.
15. In the bottom pane of the meeting select **Share** and select your Desktop to share.
16. In the bottom pane of the live event select **My desktop**.
17. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
18. In the **Microsoft Teams client** sign in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com) and sign in with the provided credentials.

19. On the left navigation pane select **Chat**.
20. Select the link sent to you by Megan Bowen to join the live event.
21. Switch back to **Client 2 VM** and select **Send live** as Megan Bowen.
22. Select **Start** to start the live event.
23. In the **Are you sure you want to start the live event now?** Window select **Continue**.
24. Switch back to **Client 1 VM** and wait for the live event to start.
25. Switch to **Client 2 VM** and select **End**.
26. In the **End live event now?** Window select **End live event**.

You have successfully created a live event and shared content with your attendees.

25.4.2 Exercise 2: Manage phone system for Microsoft Teams

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

25.4.2.1 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
3. On the left navigation pane select **Locations** and below select **Emergency addresses**.
4. Select **+ Add** from the top pane to create a new emergency address.
5. On the **Location\Add location** page, enter the following information:
   - Put in a name for your location: **Contoso Emergency Address**
   - Add a friendly description so you know why it was created: **Emergency Address for Contoso employees.**
   - Country or region: **United States**
   - Address: **1 Microsoft Way, Redmond, WA 98052**

     (You can enable **Edit the address manually**, and enter the address manually)
6. Acknowledge the emergency calling disclaimer.
7. Select **Save**.

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

25.4.2.2 Task 2 - 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
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 right to **Voicemail is available for routing inbound calls** and select **Disabled**. 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 **Manage users** from the top pane.
10. In the right-side pane, type into the search field **Megan, Alex, Joni, Lynne** and select **Add** right from their names.
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.

25.4.2.3 Task 3 - Create a call queue

Contoso 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
3. On the left navigation pane, select **Org-wide settings**, 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: **Contoso 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 **C:\Windows\Media.**

   https://github.com/MicrosoftLearning/MS-700-Managing-Microsoft-Teams/blob/master/Instructions/Labs/media/Al
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: **Contoso Call Queue**
    - You haven't added any resource accounts yet: Select **Add accounts**. On the right-side pane, search for **Contoso**, select **Add** from **Contoso Call Queue**, and then select **Add**.
    - Greeting: select **Play an audio file**, and then select **Upload file**.
    - In **Open** window, navigate to **C:\Windows\Media**, select **Alarm03.wav** and select **Open**.
    - Music on hold: **Play default music**

- Call answering: 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**
- Agents can opt out of taking calls: **On**
- Agent alert time: **30 seconds**
- Maximum calls in the queue: **50**
- When the maximum number of calls is reached: **Disconnect**
- Call time out handling: **5 minutes**
- When call times out: **Disconnect**

11. Select **Save** 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 file for demonstration purposes. In real-world scenario, you would record and prepare a greeting audio file and upload the audio file as shown in this task.

25.4.2.4 Task 4 - 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
3. On the left navigation pane, select **Org-wide settings**, 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: **Contoso Auto Attendant**
   - Username: **pilot_autoattendant1**
   - Resource Account Type: **Auto attendant**
6. Select **Save**.
7. On the left navigation pane, select **Voice** and **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: **Contoso Auto attendant**
   - Operator: **Voice app**
   - Search by resource account: **Contoso 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: **Type in the greeting message**

- Type in : **Welcome. The person you called is currently on vacation, your call will be redirected to an operator.**
- Then route the call: **Redirect call**
- Redirect to: **Voice app**
- Search by resource account: **Contoso 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: **Type in 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 **Find people** page, select **Next**.
17. On the **Resource accounts** page, select **Add accounts**. In the right-side pane, type **Contoso 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.

25.4.3 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

25.4.3.1 Task 1 – 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. Connect to the **Client 1 VM** and 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, select the **MOD Administrator**(Admin@<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. Scroll to the bottom of the page and select **Add-ons**.
6. Scroll down until you see **Microsoft 365 Domestic Calling Plan Trial** and select **Details**.
7. Select **Get 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.

25.4.3.2 Task 2 – 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Microsoft 365 admin center** and signed in as **MOD Administrator** (Admin@<YourTenant>.onmicrosoft.com).
3. Open the Navigation Menu in the upper left corner and select **Users**.
4. Select **Active users**.
5. Search for **Megan Bowen** and open the additional settings by selecting her name.
6. Select **Licenses and Apps**.
7. Under **Licenses** select **Microsoft 365 Domestic Calling Plan** by setting the checkmark in front of it.
8. Select **Save Changes** to assign the license.

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.

25.4.3.3 Task 3 – Order a phone number for your user

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

1. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. In the **Microsoft Teams client** sign in as **Joni Sherman** (JoniS@<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 Megan Bowen 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 **Location,** search **Redmond** and select **Contoso Emergency Address**.
11. For **Quantity** select 1.
12. Select **Next**, 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.

25.4.3.4 Task 4 – Assign a phone number to your user

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

1. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
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 **Megan Bowen** and select **assign**.
6. Under **Emergency Location** select **Search by the location description**.
7. Search for the emergency location you created earlier.
8. Select **Apply** to assign the phone number to the user.

END OF LAB

25.5 lab: title: 'Lab 06: Manage communication in Microsoft Teams' module: 'Module 6: Manage communication in Microsoft Teams'

26 Lab 06: - Manage communication in Microsoft Teams

27 Student lab manual

27.1 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.**

27.2 Lab Scenario

In the labs of this course you will assume the role of Joni Sherman, a Teams Administrator for Contoso Ltd. and her pilot team that shall evaluate the capabilities of Microsoft Teams in a testing environment. According to Contoso business requirements, Microsoft Teams will be used as an organization's solution for conferencing and telephony. Therefore, Teams admins need to configure conferencing functionalities, such as meetings and live event features that will provide best user experience during collaboration and communication. Furthermore, Teams admins will need to replace Contoso legacy PBX solution and configure voice features that will provide users with Teams calling capabilities.

27.3 Objectives

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

- Manage meeting policies
- Configure meeting settings
- Create live event policies
- Create a live event
- Configure emergency addresses
- Create calling policies
- Configure resource accounts and calling queues
- Create resource accounts and auto attendants
- Test configured meeting policies
- Test configured meeting settings
- Set up a Calling Plan
- Order and Assign phone numbers

27.4 Lab Setup

- **Estimated Time:** 90 minutes.

27.5 Instructions

27.5.1 Exercise 1: Manage Live event and meetings experiences

Contoso organization has deployed Microsoft 365 and is testing pilot projects on collaboration and communication scenarios to meet business requirements. First, Teams admins need to configure meeting policies and schedule initial meetings. Then, business managers want to test the Live meetings option in Microsoft Teams in order to broadcast audio and video to large audiences.

27.5.1.1 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 fulfil 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. In Microsoft Edge, sign in to **Microsoft Teams admin center** (https://admin.teams.microsoft.com) as user **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. In the **Teams admin center,** under **Meetings** section, choose **Meeting policies**.
4. Edit the **Global (Org-wide default)** policy review the available settings, and turn **Off** the **Allow cloud recording** setting.

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.

27.5.1.2 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. Open the **Microsoft Teams Desktop client**, where you are already signed in as **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft.com).
2. Select **Calendar** from the left navigation pane and **Meet Now** from the upper right corner to start a meeting.
3. On the Microsoft Teams page, leave the default settings and select **Join now** button.
4. On the Microsoft Team page, hover the mouse over the meeting page, and select the three dots (**...**) **(More actions)**.
5. Note that **Start recording** option is visible but is dimmed, not available to be selected.

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

Contoso Ltd. 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, under **Meetings** section, choose **Meetings settings**.
4. On the **Meetings settings** page, below participants, turn **Off** the option **Anonymous users can join a meeting**.

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.

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

Contoso 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 Contoso Ltd. business requirements, you will need to restrict the recording options for participants of meetings and only allow recording options to management users. Only the organizer of a live event should be able to record his own meetings.

1. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, under **Meetings** section, choose **Live event policies**.
4. Create a new **Live event policy** with the following configuration:
   - Add live events policy: **Management Live Events**
   - Description: **Recording Restriction for live events organized by managers**
   - Allow scheduling: **On**
   - Allow transcription for attendees: **Off**
   - Who can join scheduled live events: **Everyone in the organization**
   - Who can record an event: **Organizer can record**
5. Assign the new policy to the user **Megan Bowen**.

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

27.5.1.5 Task 5 – Create a new live event

Contoso Ltd. Wants to broadcast video and meeting content to large online audiences using Teams live events. As a Teams admin, you need to demonstrate the functionality of live meetings to Management.

1. Connect to the **Client 2 VM** and sign in with the Credentials that have been provided to you.
2. In the **Microsoft Teams client** sign in as **Megan Bowen** (MeganB@<YourTenant>.onmicrosoft.com).
3. Create a new live event with the title **"Management Showcase"** in a timeslot of your choice.
4. Send the attendee link to **Joni Sherman**.
5. Join the live event and share your desktop content.
6. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
7. In the **Microsoft Teams client** sign in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
8. Select the link sent to you by Megan Bowen to join the live event.
9. Switch back to **Client 2 VM** and select start the live event as **Megan Bowen**.
10. Switch back to **Client 1 VM**, wait for the live event to start and review the behavior of the live event.
11. Switch to **Client 2 VM** and **End** the live event.

You have successfully created a live event and shared content with your attendees.

27.5.2 Exercise 2: Manage phone system for Microsoft Teams

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

27.5.2.1 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane under **Locations** section, choose **Emergency addresses**.
4. Create a new emergency address with the following configuration:
   - Put in a name for your location: **Contoso Emergency Address**
   - Add a friendly description so you know why it was created: **Emergency Address for Contoso employees.**
   - Country or region: **United States**
   - Address: **1 Microsoft Way, Redmond, WA 98052**

     (You can enable **Edit the address manually**, and enter the address manually)

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

27.5.2.2 Task 2 - 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, under **Voice** section, choose **Calling policies**.
4. Edit the **Global (Org-wide default)** policy to disable **Voicemail is available for routing inbound calls** option.
5. Create a new policy with the following configuration:
   - 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**
6. Assign the new calling policy **Voicemail enabled pilot users** to users **Megan, Alex, Joni,** and **Lynne**.

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

27.5.2.3 Task 3 - Create a call queue

Contoso 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. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. On the left navigation pane, under **Org-wide settings** section, choose **Resource accounts**, and create a resource account with the following configuration:

- Display name: **Contoso Call Queue Resource Account**
- Username: **pilot_callqueue1**
- Resource Account Type: **Call queue**

3. Download the file **Alarm03.wav** from the following link and save to **C:\Windows\Media.**

   https://github.com/MicrosoftLearning/MS-700-Managing-Microsoft-Teams/blob/master/Instructions/Labs/media/Al

4. On the left navigation pane, under **Voice** section, choose **Call queues**, and create a call queue with the following configuration:
   - Call queue name: **Contoso Call Queue**
   - Add accounts: **Contoso Call Queue**
   - Greeting: **Play an audio file C:\Windows\Media\Alarm03.wav**
   - Music on hold: **Play default music**
   - Call answering: **Add groups: Sales**
   - Routing method: **Round robin**
   - Agents can opt out of taking calls: **On**
   - Agent alert time: **30 seconds**
   - Maximum calls in the queue: **50**
   - When the maximum number of calls is reached: **Disconnect**
   - Call time out handling **5 minutes**
   - When call times out: **Disconnect**

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 file for demonstration purposes. In real-world scenario, you would record and prepare a greeting audio file and upload the audio file as shown in this task.

27.5.2.4 Task 4 - 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. Connect to the **Client 1 VM** and sign in with the Credentials that have been provided to you.
2. You should still be signed in to the **Teams admin center** as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
3. On the left navigation pane, under **Org-wide settings**, choose **Resource accounts,** and create resource account with the following configuration:
   - Display name: **Contoso Auto Attendant**
   - Username: **pilot_autoattendant1**
   - Resource Account Type: **Auto attendant**
4. On the left navigation pane, under **Voice** section, choose **Auto attendants**.
5. Create a new auto attendant with the following configuration:
   - Add a name for your auto attendant: **Contoso Auto attendant**
   - Operator: **Voice app**
   - Search by resource account: **Contoso Call Queue Resource Account**
   - Time zone: **(UTC-08:00) Pacific Time (US & Canada)**
   - Language: **English (United States)**

- Enable voice inputs **Off**

6. On the **Call flow** page, configure the following:
   - First play a greeting message: **Type in the greeting message**
   - Type in: **Welcome. The person you called is currently on vacation, your call will be redirected to an operator.**
   - Then route the call: **Redirect call**
   - Redirect to: **Voice app**
   - Search by resource account: **Contoso Call Queue Resource Account**
7. 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: **Type in 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**
8. On the **Holiday call settings** page, accept the default settings.
9. On the **Find people** page, accept the default settings.
10. On the **Resource accounts** page, add the **Contoso Auto attendant**, resource account.

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

27.5.3 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

27.5.3.1 Task 1 – 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. In Microsoft Edge, sign in to **Microsoft 365 admin center** https://admin.microsoft.com as user **MOD Administrator** (Admin@<YourTenant>.onmicrosoft.com).
2. Navigate to **Billing > purchase services** and activate the **Microsoft 365 Domestic Calling Plan Trial**.

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

27.5.3.2 Task 2 – 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. You should still be signed in to the **Microsoft 365 admin center** as **MOD Administrator** (admin@<YourTenant>.onmicrosoft.com).

2. Under **Users**, select **Megan Bowen** and assign the **Microsoft 365 Domestic Calling Plan** license to her.

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.

27.5.3.3 Task 3 – Order a phone number for your user

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

1. In Microsoft Edge, sign in to **Teams admin center** (https://admin.microsoft.com) as user **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.com).
2. In **Voice,** under **Phone numbers**, **add** a new order for a phone number with the following settings:
   - Order name: **Phone number order**
   - Description: **Number for Megan Bowen during the Calling plan trial.**
   - Country or region: **United States**
   - Number type: **User (Subscriber)**
   - Location: **Contoso Emergency Address**
   - Quantity: **1**
3. Review the order and place it.

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.

27.5.3.4 Task 4 – Assign a phone number to your user

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

1. You should still be in the **Teams admin center** and signed in as **Joni Sherman** (JoniS@<YourTenant>.onmicrosoft.co
2. In **Voice,** under **Phone numbers**, select the phone number you want to assign and **edit** it.
3. Assign the phone number to **Megan Bowen** and select an **Emergency location**.

END OF LAB