Contents

1 MS-030: Office 365 Administrator

- **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 Azure 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 Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure 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 Azure 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 Azure 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-030-Office365Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

{% 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-030-Office365Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %} # GitHub User Guide for MCTs

Cloud services, such as Office 365, are updated frequently. This leads to issues for Microsoft Certified Trainers (MCTs) when they teach courses, such as MS-30: Office 365 Administrator, because lab steps change frequently as the service changes. Due to the frequency of the changes and the fact that there may not be any notification when changes occur, it can be difficult for the course development team to rapidly identify and address any lab changes.

To address these issues, we are using GitHub to publish the lab steps for courses that cover cloud services like Office 365. Using GitHub allows for collaboration between the course's authors and MCTs to keep the content current with Office 365 platform changes. Using GitHub allows the MCTs to provide feedback and suggestions for lab changes, and then the course authors can update lab steps and scripts quickly and relatively easily.

As this course is only available from an Authorized Hosting Partner, students should use the lab steps located in the online lab user interface. The hosting partner updates these labs steps dynamically as changes occur in the Office 365 user interface. Therefore, these labs steps will be as up-to-date as possible for each training session. The lab steps on GitHub are made available for you to prepare to teach this course, and for you to provide feedback to the course's authors.

When you prepare to teach these courses, you should ensure that you are using the latest lab steps by downloading the appropriate files from GitHub.

This user guide is for MCTs who are new to GitHub, and it provides steps for connecting to GitHub, downloading and printing course materials, updating the scripts that students use in labs, and explaining how you can help ensure that this course's content remains current.

Note: The lab files on GitHub are intended for MCT use only. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

2.2.1 GitHub terminology

GitHub introduces terminology that might be new to you, and the following list includes terms and concepts that this document uses. However, for a full list of GitHub terms, refer to the "GitHub Glossary" at https://help.github.com/articles/GitHub-glossary/.

Git and *GitHub*: *Git* is an open-source, change-tracking program, and *GitHub* is a site/solution built on Git. There are other websites and solutions that use Git as their backend. You would use GitHub primarily for open-source (public) development projects, and it is free for those projects. However, if you want to use GitHub for projects that are private, and not open source, you must sign up for a paid version.

Repo or *Repository*: Each project in GitHub is in a repository, or *repo*. A repo contains all of a project's files, including documentation, and it supports revision history. A repository can be public or private, and you can have a local copy of the repo on your computer hard drive, or you can use the repo within GitHub.

Markdown: This is a text-file format that you can use for creating documentation. It is text-based and very simple to update, which makes it easy to use during collaboration. GitHub then renders it as HTML.

GitHub flavored markdown (GFM): There are many variations, or flavors, of the Markdown file format. The GitHub version, commonly referred to as *GFM*, is one of the most common variations of Markdown. For more information about GFM and how you can use the Markup format for your GFM documents, refer to "Getting started with writing and formatting on GitHub" at https://help.github.com/articles/getting-started-with-writing-and-formatting-on-github/.

Fork: This is a copy of another repo that resides in your GitHub account, in comparison to a *branch*, which lives in the original repo. See "Branch" directly below.

Branch: This is a copy of a repository that resides in the same repository as the original. You can merge a branch with the original.

Fetch: This is the process of retrieving a copy of the latest changes from an online repo. However, a fetch *does not* merge changes.

Pull: This is the process of fetching the latest changes from an online repo and merging them with local changes.

Merge: This is the process of fetching changes from one branch and applying them to another. This includes retrieving changes from an online repo, and then applying them to that repo's local version.

Pull request: This is a set of proposed changes to a repo that a user submit, and a repo's owners or collaborators then can accept or reject the pull request.

Push: This is the process of sending or submitting your local changes to the online repo.

Collaborator: This is a GitHub user that has permissions to add, delete, or change a repo's content.

2.3 Overview of Microsoft Learning's GitHub solution for course labs

The Microsoft Learning team has created a solution that allows them to publish updated lab and lab answer keys (LAKs) and updated lab scripts regularly to GitHub. The solution also includes a script and tools that you can use to print labs and lab answer keys from Microsoft Word .docx files. However, if you want to use this solution, you must perform several steps the first time that you download and print lab files. A later section of this file details these steps, which include that you must:

1. Sign-up for a GitHub account.
2. Install the GitHub Desktop.
3. Install the prerequisite software:

- Pandoc version 1.19.2
- Windows PowerShell Community Extensions

Once you sign up for GitHub and install the prerequisite software, the steps for downloading and printing the course-lab materials are the same for each course.

You can use a variety of tools that support Git with GitHub, including Microsoft Visual Studio, Visual Studio Code, or any of the Git command-line tools that are available online.

> **Note:** GitHub has a desktop client and a command-line interface. Throughout this document, we use the desktop client. If GitHub and Git are new concepts, and you would like a more in-depth

introduction, refer to the "GitHub Hello World guide" at https://guides.github.com/activities/hello-world/.

2.4 Prerequisites

The following section details the prerequisites for using GitHub and the Microsoft Learning courseware lab solution.

2.4.1 Signing up for a GitHub account

In order to clone a repo or collaborate with Microsoft Learning on GitHub, you need to sign up for a GitHub account.

To sign up for a GitHub account, perform the following steps.

1. In your browser, navigate to https://GitHub.com/.
2. In the **Username** text box, enter a unique user name.
3. In the **Email** text box, enter your email address.
4. In the **Password** text box, enter a password that meets GitHub's complexity requirements.
5. Click **Sign up for GitHub**.
6. On the **Join GitHub** page, select **Create an account**.
7. Verify that **Free** is selected and select **Continue**.
8. On the Welcome GitHub page, complete the form and select **Submit** or select **skip this step**.

GitHub will send a confirmation email to the email address that you provide. You must open the email, and then click **Verify email address**.

2.4.2 Installing GitHub Desktop

GitHub Desktop provides a graphical user interface (GUI) for GitHub, and you can use it to perform most common functions. There are some operations that you can perform only from a command line, but none of these operations are necessary for downloading and printing lab files.

To install the GitHub Desktop, perform the following steps:

1. In your browser, navigate to https://desktop.GitHub.com.
2. Click **Download for Windows**.
3. When the **GitHubDesktopSetup.exe** file has downloaded, double-click the file to start the setup, or click **Run** if you receive a prompt from Internet Explorer.
4. In the **Application Install - Security Warning** dialog box, click **Install**.
5. Close GitHub Desktop.

2.4.3 Installing Pandoc version 1.19.2

Pandoc is a tool that you can use to convert files from one format to another. It can read many formats, including GFM, and you use it output Microsoft Word's .docx format. Pandoc is the tool behind the scripts that Microsoft Learning provides to create Word documents from the Markdown file format of the lab files. If you do not install Pandoc, the document-creation script fails.

To install Pandoc, perform the following steps:

1. In your browser, navigate to https://GitHub.com/jgm/pandoc/releases/tag/1.19.2.
2. Select **pandoc-1.19.2-windows.msi**.
3. When the **pandoc-1.19.2-windows.msi** file has downloaded, double-click the file to start the setup, or click **Run** if you receive a prompt from Internet Explorer.
4. In the **Pandoc 1.19.2 Setup** dialog, review the License Agreement, select **I accept the terms in the License Agreeement**, and then click **Install**.
5. Click **Finish**.

2.4.4 Installing PowerShell Community Extensions

PowerShell Community Extensions (PSCX) is an open-source project that extends Windows PowerShell with scripts, cmdlets, functions, and other features. You use PSCX to create the .zip files that contain your .docx files. Please note, if you do not install these extensions, the document-creation script fails.

To install PSCX, perform the following steps:

1. Open Windows PowerShell as an administrator
2. In the script window enter the following command and press enter:

```
Install-module PSCX
```

3. If prompted that you are installing a module from an untrusted repository, select **Yes**.

   Important: After you install Pandoc and PSCX, you must restart your computer to complete the installation. If you do not restart your computer, the document-creation script might fail.

2.5 Downloading and printing lab files

The labs are stored on GitHub in a repo. The structure for each Microsoft Learning course repo is similar, and each contains the following folders:

- **Allfiles:** This folder contains any supporting files for the labs. This is the same as the Allfiles folder that would appear on the virtual hard disk for virtual machines (VMs).
- **Build**: This folder contains the Windows PowerShell script and supporting files for creating Word documents from the lab files that are in the Markdown format.
- **Instructions:** This folder contains the lab files and LAK files, which are in the Markdown format.

You need all of these folders if you want to print the lab files.

2.5.1 Downloading the latest materials for course labs

If you want to build Word documents from Markdown files, you must clone or fetch a copy of the repo on your local computer. If you want to clone the files, you must know the GitHub location of the course files. You can use the **Search GitHub** search box on the GitHub home page to search for these files by using the course number. You also can browse through the repos under the Microsoft Learning organization page on GitHub. The Microsoft Learning page on GitHub is located at https://github.com/MicrosoftLearning/.

2.5.1.1 To clone the course repo to your local machine

1. In your browser, navigate to the online repo in GitHub.
2. On the **repo** page, click **Clone or download**.
3. In the **Clone with HTTPS** dialog box, click **Open in Desktop**.
4. In the **Internet Explorer** confirmation dialog box, click **Allow** (or the equivalent for your browser).
5. Switch to GitHub Desktop.
6. In the **Browse For Folder** dialog box, select a folder as the root for the local repo, and then click **Ok**.

If you plan to clone several repos, you can choose one common folder in this step. This creates a subfolder for each repo.

7. In the **Repositories** list, right-click the repository name, and then click **Open in Explorer** to view the local files.

After you clone a repo the first time, on subsequent visits, you can open GitHub Desktop, select the repository, and then click **Sync** to retrieve the latest files.

> **Note:** For more information about synchronizing your repo, refer to Working with your remote repository on GitHub or GitHub Enterprise at https://help.github.com/desktop/guides/contributing/working-with-your-remote-repository-on-github-or-github-enterprise/.

2.5.2 Printing the lab and LAK files

If you want to print lab and LAK files, you must convert them Word documents first. Microsoft Learning has a Windows PowerShell script that automates this task. The script creates the Word documents, and then packages the Word documents into .zip files. At the same time, it creates a .zip file that contains the lab's supporting files such as scripts and text files, which you will need when you set up your lab environment.

The Windows PowerShell script, Pandoc.ps1, is in the **\Build** folder. The folder also contains template.docx, which the script uses to format files in Word. Do not alter the template.docx file.

2.5.2.1 To convert the lab files and create the Zip packages:

1. In **File Explorer** navigate to the \Build folder in the repo you cloned, such as

```
..\Documents\GitHub\MS-30: Office 365 Administrator-EnablingAndManagingOffice365\Build
```

2. Right-click the file **pandoc.ps1**, and click **Run with PowerShell**.
3. In the **Windows Powershell** window, if you recieve an **Execution Policy Change** prompt, type **Y** and then press Enter.
4. When you receive the **What is the current version?** prompt, enter a short string or number to uniquely identify the Zip files that is built,

   Note: The **current version** string will be added to the name of the Zip file.
5. Switch to File Explorer and in the **\Build folder**, select the .zip files that you just created. The file names will be **allfiles-v*version*.zip** and **lab_instructions-v*version*.zip**
6. Move these files to a new location to avoid accidentally attempting to add them to the repo as part of a pull request.

   Note: To avoid receiving the **Execution Policy Change** prompt, you can change the **Set-ExecutionPolicy** setting in Windows PowerShell to execute scripts without restriction. After changing the **ExecutionPolicy** property, be aware now scripts that you run have the power to make disruptive things happen to your computer.

2.5.2.2 To print the lab files:

- Open the lab files in Microsoft Word, and then print them by using the Word print functionality.

2.6 Receiving update notifications, suggesting changes, and collaborating on projects

You can configure your GitHub experience so that you receive notifications when updates occur to a GitHub repo. There are several ways in which you can sign up for notifications, and many of them relate to the many ways that you can collaborate on a project. To receive notifications, you can:

- *Watch repositories*: When you watch a repository, GitHub subscribes you automatically to notifications for any new pull requests or issues that are created for that specific repository. You automatically watch any repository that you create or for which you are a collaborator.
- *Pull request*: When you create a pull request, and propose that the owners of a repo accept a change that you make, you automatically subscribe to receive notifications for the related discussion about the pull request. In order to create a Pull request you must first create a branch.
- *Comments*: When you make comments about another person's pull request, GitHub subscribes you automatically to the forum that pertains to that comment, or you can subscribe to the forum manually.
- *Issues*: An issue is a suggestion, question, or request that pertains to a repository. Each issue has its own discussion, and you can subscribe to issues, or GitHub subscribes you automatically to issues that you create.
- *Mentions*: When another user mentions you in a conversation, using your GitHub user name (@*username*), GitHub subscribes you automatically to the discussion.

You can modify how and when you receive notifications, and you also can unsubscribe to any or all discussions.

2.6.1 Watching a repo

The simplest way to make sure you know about any changes to a repo is to **watch** it. You can do that, even if you do not clone a local copy of the repo.

To watch a repo, perform the following steps:

1. In Internet Explorer, navigate to the repo on GitHub.
2. Click **Watch**, and then under **Notifications**, select **Watching**.

To quit watching a repo, perform the following steps:

1. In Internet Explorer, navigate to the repo on GitHub.
2. Click **Watch**, and then under Notifications, select **Not watching**.

   Note: You can select the **Ignoring** option under the **Watch** drop-down list. However, this means that you receive *no* notifications, even if another user includes you in a discussion with the mention functionality and your GitHub user name. Therefore, you should be careful configuring the **Ignoring** option.

2.6.2 Suggesting changes and collaborating on a repo

GitHub makes it easy to collaborate with other Microsoft Learning users on the courses in which you are interested.

You can modify your own copy of the lab materials, and then submit your changes to Microsoft Learning so that they can incorporate your updates. You might want to modify your lab materials if:

- You find a mistake in a lab.
- The UI has changed since the lab was created.
- You think that the lab needs improvements or modifications.

To modify lab materials, you should branch the repo, make updates in your branch, and then submit a pull request to the main (master) branch. This allows Microsoft Learning staff, and other MCTs and GitHub users to review, and comment on, your changes.

You can review and comment on changes that other users make, and Microsoft Learning staff then approves and merges these changes into the master branch. This action notifies any user who is watching the repo that a change has occurred.

2.6.2.1 To create a repo branch:

1. In Internet Explorer, navigate to the repo on GitHub.
2. Click **Branch : *branchname***, and then from the **Branches** list, select the branch you want to copy.
3. If there is only one branch, the **Branch** drop-down list shows **Branch: master**, and the only branch that is available is **master**.
4. In the blank text box, type the name of the branch that you want to create.
5. Click **Create branch: *new branch name*** when it appears.

2.6.2.2 To delete a repo branch:

1. In Internet Explorer, navigate to the repo on GitHub.
2. Click ***n* branches**, where ***n*** is the number of existing branches.
3. On the **Branches** page, in the row for the branch that you want to delete, click **Delete this branch** icon.

After you have created a Branch, you can clone the files to your local repo, update them on your computer, and then check in the changes from the GitHub Desktop. If you are working with Markdown or other text files, you can edit them in GitHub, and then check in the changes online.

2.6.2.3 To commit changes by using GitHub Desktop:

1. Open GitHub Desktop.
2. Select the repo that contains your changes, and then click **Changes**.
3. Select the changes that you want to commit, and then in the **Summary** text box, write a short description of the change.
4. In the **Description** text box, write a more-detailed description of the change, if necessary.
5. Click **Commit to master**, and then click **Sync** to push the local changes to the online repo.

2.6.2.4 To edit files and commit changes in the online repo:

1. In Internet Explorer, navigate to the applicable repo on GitHub, and then select the file that you want to edit.
2. Click the **Edit this file** icon.
3. Make your changes in the **Edit file** tab of the webpage, and then click **Preview changes** to view your proposed changes, without committing them.
4. Under **Commit changes**, in the **Update *filename*** text box, enter a short description of the changes.
5. In the **Add an optional extended description...** text box, enter a more detailed description of the change, if necessary, and then click **Commit changes**.

2.6.2.5 To create a pull request:

1. In Internet Explorer, navigate to the applicable repo on GitHub.
2. Click **Branch:*branchname***, and then in the **Branches** list, select the branch for which you want to create a pull request.
3. Click **New pull request**, and then on the **Open a pull request** page, in the **Title** text box, update the name of the pull request, if necessary.
4. On the **Write** tab, in the **Leave a comment** text box, provide a description of the proposed change, and then click **Create pull request**.

As we noted previously, you also can comment on pull requests and proposed changes (commits) that other users make. When you comment on a commit, you view a source diff of the file, and you then you can comment on specific changes on a line-by-line basis or on the entire commit.

2.6.2.6 To review and comment on a pull request:

1. In Internet Explorer, navigate to the applicable repo on GitHub.
2. Click **Pull requests *n***, where ***n*** is the number of active pull requests.
3. Select the pull request that you want to review, and then on the **Write** tab, in the **Leave a comment** text box, input your comment.
4. Click **Comment**.

2.6.2.7 To review and comment on a commit:

1. In Internet Explorer, navigate to the repo on GitHub.
2. Click ***n* commits**, where ***n*** is the number of commits that have been submitted. If you want to review the latest commit, you can select the title/short description of the commit from file list.
3. In the **source diff** section, select the change on which you want to comment by clicking the plus sign (+) that appears when the mouse hovers over the applicable change.
4. On the **Write** tab, in the **Comment** text box, provide your comment.
5. Click **Comment**.

If you wish to provide an overall comment on the commit, under ***n* comments on commit**, where ***n*** is the number of comments submitted, and then under the **Write** tab, in the **Leave a comment** text box, type your comment, and Click **Comment on this commit**.

You also can make suggestions about an overall project, by submitting an Issue or commenting on an existing Issue.

2.6.2.8 To submit an Issue:

1. In Internet Explorer, navigate to the applicable repo on GitHub.
2. Click **Issues**, and then click **New issue**.
3. In the **Title** text box, enter the title for the issue, and then in the **Leave a comment** text box, type a description of the issue or suggestion.
4. Click **Submit new issue**.

2.6.2.9 To review and comment on an existing issue:

1. In Internet Explorer, navigate to the applicable repo on GitHub.
2. Click **Issues**, and then select the title of the issue that you want to review.
3. On the **Issue name** page, on the **Write** tab, in the **Leave a comment** text box, type your comment.
4. Click **Comment**.

   Whenever you create an issue, or a comment on a pull request or commit, you also can include other GitHub users or teams into the conversation by performing a **mention** of them in the comment's body. If you are familiar with Twitter, this feature will look very familiar.

2.6.2.10 To mention a GitHub user in a comment:

1. In Internet Explorer, navigate to the applicable repo on GitHub.
2. Create your comment or issue, as described previously, and then in the **comment** text box, type **@**, followed by the user or team name, within the comment.

   Note: When you type the **@** symbol, a list appears that contains GitHub users who are collaborators on the applicable project and anyone who is participating in the project's comments. The list uses autocomplete as you type, so that you can filter the list easily.

2.7 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.

4 Module 1 - Lab 1 - Initialize your Microsoft 365 Tenant

Adatum Corporation runs their legacy applications (such as Microsoft Exchange) in an on-premises deployment. However, they recently subscribed to Microsoft 365, thereby creating a hybrid deployment in which they must synchronize their on-premises and cloud deployments.

Throughout the labs in this course, you will take on the persona of Holly Dickson, Adatum's Enterprise Administrator. You have been tasked with deploying Microsoft 365 using a virtualized lab environment. Adatum's project team has decided to implement Microsoft 365 in a pilot project that will not only provide them with experience using the product, but also enable them to match their business requirements with the Microsoft 365 feature set. In this exercise, you will begin implementing Microsoft 365 within the pilot project by setting up Adatum's Microsoft 365 trial tenant.

Your instructor will provide guidance on how to obtain your Microsoft 365 credentials in your lab-hosted environment. You will use these credentials throughout the remaining labs in this course.

In your lab environment, your lab hosting provider has already:

- Deployed the trial tenant
- Created a default tenant administrator account (known as the MOD Administrator)
- Created 9 additional user accounts
- Created a custom domain in Microsoft Azure (not on-premises)
- Created the DNS records in Microsoft Azure that are required to support the custom domain and the selected Microsoft 365 services

In this lab, you will complete the following exercises:

- Exercise 1 - Provision Adatum's Microsoft 365 tenant
- Exercise 2 - Complete the custom domain setup process
- Exercise 3 - Explore the Microsoft 365 administrator interfaces

4.1 Exercise 1 - Provision Adatum's Microsoft 365 Tenant

In this exercise, you will update Adatum's Microsoft 365 organizational profile, and you will verify the provisioning of Adatum's Microsoft 365 tenant, as well as the tenant's service health.

4.1.1 Task 1 - Obtain Your Microsoft 365 Credentials

Once you launch the lab, a free trial tenant will be automatically created for you to access Azure in the Microsoft Virtual Lab environment. This tenant will be automatically assigned a unique Microsoft 365 administrator account and password. You must retrieve this username and password so that you can sign into Azure within the Microsoft Virtual Lab environment.

1. Because this course can be offered by learning partners using any one of several authorized lab hosting providers, the actual steps involved to retrieve the UPN name, network IP address, and tenant ID associated with your tenant may vary by lab hosting provider. Therefore, your instructor will provide you with the necessary instructions on how to retrieve this information for your course.

    You should write down the following information (provided by your instructor) for later use:

    - **Tenant suffix ID.** This ID is for the onmicrosoft.com accounts that you will use to sign into Microsoft 365 throughout the labs. This is in the format of **{username}@M365xZZZZZZ.onmicrosoft.com**, where ZZZZZZ is your unique tenant suffix ID provided by your lab hosting provider. Record this ZZZZZZ value for later use. When any of the lab steps direct you to sign into the Office 365 or Microsoft 365 portals, you must enter the ZZZZZZ value that you obtained here.

- **Tenant password.** This is the password for the admin account provided by your lab hosting provider.

4.1.2 Task 2- Set up the Organization Profile

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have been tasked with setting up the company's profile for its Microsoft 365 trial tenant. In this task, you will configure the required options for Adatum's tenant. Since Holly has yet to create a personal Microsoft 365 user account (you will do this in Lab 2), she will initially sign into Microsoft 365 as the default Microsoft 365 MOD Administrator account using the Tenant admin's username and password that was assigned to it by your lab hosting provider.

1. When you open your lab hosting provider's Virtual Machine environment, you need to begin with the Domain Controller VM (LON-DC1). If your VM environment opens with one of the other virtual machines, such as LON-CL1, then switch to the **LON-DC1** VM.
2. Log into LON-DC1 as the **Administrator** with the password **Pa55w.rd**.
3. If you receive a **Networks** warning message asking if you want this PC to be discoverable by other PCs and devices on this network, select **Yes.**
4. **Server Manager** will automatically start. Leave it open but minimize the window for now.
5. On the taskbar at the bottom of the page, select the **Microsoft Edge** icon. Maximize your browser window when it opens.
6. In your browser go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**
7. In the **Sign in** dialog box, copy and paste in (or enter) the username of the Microsoft 365 Tenant administrator account provided by your lab hosting provider (**admin@M365xZZZZZZ.onmicrosoft.com**, where ZZZZZZ is your unique tenant suffix ID provided by your lab hosting provider) and then select **Next**.
8. In the **Enter password** dialog box, copy and paste in the **Tenant Password** provided by your lab hosting provider and then select **Sign in**.
9. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
10. If a **Get your work done with Office 365** window appears, then close it now.
11. In the **Microsoft Office Home** page, you are now signed in as the **MOD Administrator** account (note the **MA** initials in the circle that appears in the upper right-hand corner of the screen). The MOD Administrator is a pre-defined user created in Microsoft 365 by your lab hosting provider. Since this user has been assigned a Microsoft 365 administrator role (in this case, the Global Admin role), the Microsoft 365 admin center is available on the home page along with all the other Office apps.

    On the **Office 365 Home** page, the list of available apps is displayed. If an **Office 365 apps** box appears on the screen, select the **Got it!** button to close the box, since it covers up several of the apps. Select the **Admin** app, which opens the **Microsoft 365 admin center**.
12. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **...Show all** to display all the navigation menu options.
13. In the left-hand navigation pane, select **Settings**, and then in the **Settings** group, select **Org Settings**.
14. In the **Settings** window, the **Services** tab is displayed by default at the top of the screen. Since you want to update the organization profile, select the **Organization profile** tab, and then in the list of organization settings, select **Organization information**.
15. In the **Organization information** window that appears, enter the following information:
    - Name: Replace **Contoso** with **Adatum Corporation**

    Note: The Contoso organization name was explained in the Introduction section at the start of this lab. For the purposes of this lab, you will change it to Adatum Corporation.

    - Street address: **123 Main Street**
    - City: **Redmond**
    - State or province: **Washington**

- ZIP or postal code: **98052**
- Country or region: **United States**
- Phone: **425-555-1234**
- Technical contact: **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
- Preferred language: **English**

16. Select **Save**.
17. Once the changes have been saved, a **Saved** message will appear at the top of the **Organization information** window. Select the **X** in the upper right-hand corner of the window to close it.
18. This will return you to the **Organization profile** tab of the **Org settings** window. In the organization profile list, select **Release preferences**.
19. In the **Release preferences** window, select **Targeted release for select users** and then select **Save**.

    Note: One of the benefits of Microsoft 365 is the ability to have the latest features and updates applied to your environment automatically, which can reduce maintenance costs and overhead for an organization. By setting up your Release preferences, you can control how and when your Microsoft 365 tenant receives these updates.

    The **Targeted release for select users** option enables you to create a control group of users who will preview updates so that you can prepare the updates for your entire organization. The **Targeted release for everyone** option is more commonly used in development environments, where you can get updates early for your entire organization. In non-development environments, such as Adatum, targeted release to select people is the more typical preference as it enables an organization to control when it wants to make updates available to everyone once the updates have been reviewed by the control group.
20. Under the **Targeted release for select users** setting are options to **Select users** and **Upload users** (from a CSV file). Select the **Select users** option.
21. In the **Choose users for targeted release** window, select the **Who should receive targeted releases?** field. This will display the list of existing Microsoft 365 user accounts that were created in your Microsoft 365 tenant by your lab hosting provider.
22. In the list of users, scroll down and select the **MOD Administrator** account and then select **Save**.
23. On the **Release preferences** window, select the **X** in the upper right-hand corner to close the window.
24. On the **Organization profile** tab of the **Org settings** window, select **Custom themes**.
25. In the **Custom themes** window, scroll though the page and review the various theme and branding options that are available for you to update. For the purpose of this lab, you can change any of the options or leave the default values as is. For example, you can add the logo of your company and set the background image as the default for all your users. Along with these options you can change the colors for your navigation pane, text color, icon color, and accent color. Go ahead and explore the different options for your tenant and make any changes that you wish.

    Note: Some color patterns aesthetically distract users. If you do change any of the colors, it is recommended that you avoid using high contrasting colors together, such as neon colors and high-resolution colors like bright pink and white.
26. If you made any changes in the **Custom themes** window, select **Save** when you are done. When you are finished with the **Custom themes**, select the **X** in the upper right-hand corner to close the window.
27. Remain logged into the LON-DC1 VM and leave all the tabs open in your browser for the remaining tasks in this lab exercise.

4.1.3 Task 3: Confirm Microsoft 365 Tenant provisioning

While your lab hosting provider created Adatum's Microsoft 365 tenant, Adatum must still configure and provision it. In your role as Holly Dickson, Adatum's Enterprise Administrator, you will complete the provisioning process in this task so that you can proceed with your Microsoft 365 pilot project.

1. After completing the previous task, you should still be logged into **LON-DC1** as the **Administrator** account, and you should be signed into the **Microsoft 365 admin center** as the **MOD Administrator** account.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users**, and then in the **Users** group, select **Active users**.
3. In the **Active users** list, you will see the list of existing Microsoft 365 user accounts that were created by your lab hosting provider.

   Review the **Username** column. Note that each user's username is assigned to the **M365xZZZZZZ.onmicrosoft.com** domain (where ZZZZZZ is tenant ID assigned to your Microsoft 365 tenant).

   To confirm that these users have been licensed, review the **Licenses** column. Each user should be assigned an **Office 365 E5** license and an **Enterprise Mobility+Security E5** license. The MOD Administrator account should also be assigned a **Windows 10 Enterprise E3** license.
4. In the left-hand navigation pane, under the **Admin centers** section, select **Exchange**.
5. A new tab will open in your browser displaying the **Exchange admin center**. In the left-hand navigation pane, select **recipients**.
6. On the **recipients** page, the **mailboxes** tab at the top of the page is displayed by default. This displays the existing Microsoft 365 user mailboxes. The same users who were displayed in the **Active users** list in the **Microsoft 365 admin center** should be displayed in the **mailboxes** tab.

   If you see the same list of users, this confirms the fact that your Microsoft 365 tenant had been properly provisioned and does not have any issues at this time.
7. In your browser, close this **Exchange admin center** tab but leave the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab open and proceed to the next task.

4.1.4 Task 4: Verify Microsoft 365 service health

In this task, you will determine the service health of your Microsoft 365 tenant.

1. After completing the previous task, you should still be logged into **LON-DC1** as the **Administrator** account, and you should be signed into the **Microsoft 365 admin center** as the **MOD Administrator** account.
2. In the **Microsoft admin center**, in the left-hand navigation pane, select **Health**, and then select **Service health**. This will display the **Service health** dashboard.
3. On the **Service health** page, the **All services** tab at the top of the page is displayed by default. This tab displays all the Microsoft 365 services that are available with your current subscriptions.

   Review the **Status** column for each service. If any service has a status other than **Healthy**, select the **status** for that service (the status value is hyperlinked, whereas the service name itself is not).
4. Selecting the status of an non-healthy service displays the **Advisories** tab at the top of the page. Review any service interruption records or additional information in this **Advisories** tab.

   Note: During Microsoft testing, on rare occasions Microsoft 365 did not create the trial tenant properly; as a result, the tenant did not have all the services available to it. If this happens to you, you should create a new trial tenant using a different business email (Microsoft account).
5. After reviewing the advisories for the selected service, select the **All services** tab at the top of the page. Repeat steps 3-4 for any other services that do not have a **healthy** status.
6. Leave your web browser open and proceed to the next lab exercise.

Results: After completing this exercise, you should have successfully provisioned the Microsoft 365 tenant account for A. Datum Corporation.

4.2 Exercise 2: Complete the Custom Domain Setup process

Adatum has purchased a new domain (provided by your lab hosting provider) that resides in Microsoft Azure and not on-premises. To support Adatum's new custom domain, your lab hosting provider took on the role of Adatum's third-party domain registrar. In doing so, it added the custom domain, as well as the DNS records that are necessary to support the services required by Adatum for this new domain.

Most companies do not personally manage their DNS records themselves; instead, they have a third-party resource that manages these records for them. To assist in this effort, Microsoft 365 provides certain third-party domain registrars with an automation tool that automatically adds and replaces a company's DNS records. The automation tool also federates the sign in credentials for the third-party registrars and Microsoft 365.

Using a tool to automatically maintain DNS records is a much-welcomed improvement from the days when companies had to manually maintain these records, which oftentimes introduced human error into a rather complicated process. Because these tools eliminate the need to manually add the DNS records, they eliminate human error from the process.

Even though your lab hosting provider created the custom domain and corresponding DNS records in Microsoft Azure, Adatum must still complete the provisioning of this custom/vanity domain and its DNS records. This process is important since it places Adatum's business' name as its email domain, which adds validity to message traffic and confirms that Adatum owns the vanity domain that it has added.

To complete the domain setup process, you must run a setup wizard that verifies the accuracy of each required DNS record. This process enables you to review and validate the different types of DNS records that have been added to support this new vanity domain in Adatum's Microsoft 365 deployment.

4.2.1 Task 1: Complete Adatum's custom domain setup

Your lab hosting provider has already added a custom domain for Adatum; however, it did not complete the custom domain setup process. In this task you will complete the setup of this custom domain in Microsoft 365. Your lab hosting provider has added the necessary DNS records for Adatum; it is your job to complete this setup process by initiating a wizard that verifies the accuracy of these DNS records.

1. After completing the previous lab exercise, you should still be logged into **LON-DC1** as the **Administrator** account.

2. In your Microsoft Edge browser, you should still be logged in to Microsoft 365 as the **MOD Administrator** (**admin@M365xZZZZZZ.onmicrosoft.com**). You should have tabs open for the Microsoft Office Home page and the Microsoft 365 admin center.

3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, you already expanded the **Settings** group in the previous exercise when you updated the **Org settings**. To complete the custom domain setup in this task, select **Domains** that appears within the **Settings** group.

4. On the **Domains** page, you should see two domains.

   One is the **M365xZZZZZZ.onmicrosoft.com** domain, which was automatically created for Adatum's Microsoft 365 tenant (where ZZZZZZ is your unique tenant ID).

   The other domain is the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain, which is the custom vanity domain that was created for Adatum by your lab hosting provider.

   Important: The **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain should be set as Adatum's Default domain (note the **Default domain** moniker next to the domain name). If your lab hosting provider set the **M365xZZZZZZ.onmicrosoft.com** domain as Adatum's default domain, you must change it so that **xxxUPNxxx.xxxCustomDomainxxx.xxx** is the default domain. Having this domain set as the default domain will come into play later in this course when you perform directory synchronization.

   Therefore, if the **M365xZZZZZZ.onmicrosoft.com** domain is set as the default domain, select the vertical ellipsis icon that appears to the right of the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and then select **Set as default** on the menu that appears. In the **Set this domain as default?** dialog box that appears, select the **Set as default** button.

   Before you proceed, verify the **xxxUPNxxx.xxxCustomDomainxxx.xxx** custom domain is set as the Default domain.

5. In the list of domains, note the **Status** of the custom domain, which is **Incomplete setup**. Select the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain, which opens the setup page for this domain.

6. On the custom domain's setup page, note that only one tab currently appears, which is the **Overview** tab. Once you finish provisioning this domain, a second tab titled **DNS records** will appear. You will see this tab towards the end of this task.

   Select the **Continue setup** option on the menu bar at the top of the page. This will initiate the **Add domain** wizard. Since the custom domain has already been added, by selecting the **Continue setup**

option the wizard will skip to the steps on connecting your domain.

7. On the **How do you want to connect to your domain?** page, select **More options**. This displays two options - **Add your own DNS records**, and **Skip and do this later (not recommended)**. The **Add your own DNS records** option is selected by default. Select the **Continue** button, which opens the **Add DNS records** page.

8. The **Add DNS records** page identifies the services that an organization can implement in its Microsoft 365 deployment that require DNS records. Your lab hosting provider has taken on the role of a third-party registrar for Adatum. In doing so, it created in your lab environment each of the DNS records that are required for all the services on the **Add DNS records** page. The check box for the **Exchange and Exchange Online Protection** services should be selected by default (if not, select it now).
   Three DNS records are required to implement these Exchange services - an **MX** record, a **CNAME** record, and a **TXT** record. Select each record to expand it, and then note the information required for each record.

9. At the bottom of the **Add DNS records** page select **Advanced Options**.

10. Two additional services are displayed under the **Advanced Options** section: **Skype for Business** and **Intune and Mobile Device Management for Microsoft 365**.
    Select the check box for each of these two services. This will display the DNS records required for each service.

11. Note that four DNS records are required to implement **Skype for Business** - two **CNAME** records and two **SRV** records. Select each record type to expand it and then note the information required for each record.

    Important: Even though Adatum is using Microsoft Teams for online communication services such as chat, conference calls, and video calls, you must still select the **Skype for Business** check box. The reason for this is that Teams requires the same two SRV records required by Skype for Business. Without these two SRV records, Adatum's users will not be able to make outbound calls from within Teams (or Skype for Business). Since your lab hosting provider created these SRV records, you want to select this **Skype for Business** check box so that the wizard validates the accuracy of these two SRV records that will be used by Microsoft Teams.

12. Note that two CNAME records are required to implement **Intune and Mobile Device Management for Microsoft 365**. Select the **CNAME** record to expand it, and then note the information required.

13. Select the **Continue** button at the bottom of the page. By selecting this button, the wizard will validate whether the DNS records were properly set up.

14. If the DNS records were correctly set up by your lab hosting provider, the **Domain setup is complete** page should appear. Select **Done**.

15. You will be returned to the custom domain page, which will display the **Overview** tab. The **Domain status** should now display **Healthy**.

```
Note how a second tab titled **DNS records** now appears next to the **Overview** tab on this page. Sel
```

16. You have now completed the setup of Adatum's new vanity domain. However, as a best practice, there is one final step that you should perform. You should maintain a documented history of the DNS records that were created for Adatum by its domain registrar (your lab hosting provider) in the event you ever need to reference this information in the future.
    To do so, on the **DNS records** tab, select the **Download CSV file** option. If a notification bar appears, select **Save**.

17. On the taskbar at the bottom of your screen, select the **File Explorer** icon.

18. In **File Explorer**, select the **Downloads** folder in the tree pane, and then double-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx.csv** file that was just downloaded. Select **Notepad** to open the file.

19. Review each of the records that were created for each DNS record type.

20. Close Notepad and File Explorer.

21. Leave your web browser open along with the Microsoft Office Home tab and the Microsoft 365 admin center tab and proceed to the next lab exercise.

Results: After completing this exercise, you should have successfully completed the setup process for Adatum's custom vanity domain.

4.3 Exercise 3 - Exploring the Microsoft 365 administrator interfaces

Now that you have finished provisioning your Microsoft 365 tenant, you can begin using Microsoft 365. In this exercise, you will be guided through several of the more commonly used Microsoft 365 administrator interfaces to familiarize yourself with them.

In the prior exercises, you accessed the Microsoft 365 admin center from the domain controller (LON-DC1) as you finished provisioning your Microsoft tenant and set up Adatum's custom domain. In this exercise, you will switch to the client PC on LON-CL1 to explore the Microsoft 365 administrator interfaces.

4.3.1 Task 1 - Explore the Microsoft 365 admin center

While you have already been introduced to the Microsoft 365 admin center in the prior lab exercises, in this task you will examine some additional functionality within this portal.

1. Switch to the **LON-CL1** client VM.
2. Log into LON-CL1 as the **Administrator** with the password **Pa55w.rd**.
3. If you receive a **Networks** warning message asking if you want this PC to be discoverable by other PCs and devices on this network, select **Yes.**
4. On the taskbar at the bottom of the page, select the **Microsoft Edge** icon. Maximize your browser window when it opens.
5. In your browser go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**
6. In the **Sign in** dialog box, copy and paste in (or enter) the username of the Microsoft 365 Tenant administrator account provided by your lab hosting provider (**admin@M365xZZZZZZ.onmicrosoft.com**, where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and then select **Next**.
7. In the **Enter password** dialog box, copy and paste in the **Tenant Password** provided by your lab hosting provider and then select **Sign in**.
8. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
9. If a **Get your work done with Office 365** window appears, then close it now.
10. In the **Microsoft Office Home** page, you are now signed in as the **MOD Administrator** account (note the **MA** initials in the circle that appears in the upper right-hand corner of the screen).

    On the **Office 365 Home** page, the list of available apps is displayed. If an **Office 365 apps** box appears on the screen, select the **Got it!** button to close the box, since it covers up several of the apps. Select the **Admin** app, which opens the **Microsoft 365 admin center**.
11. In Exercise 1, you already viewed the **Active Users** within the **Microsoft 365 admin center**. In this task, you will continue your exploration of Microsoft 365 clients by viewing the Microsoft 365 groups. In the left-hand navigation pane, select **Groups** and then select **Active groups**. This will display the two groups that were created by default for Adatum's Microsoft 365 tenant.
12. In the left-hand navigation pane, select **...Show all** to display all the navigation menu options.
13. In the left-hand navigation pane, expand **Health** and then select **Message center**.
14. In the **Message center** window, the **All active messages** tab is displayed by default. Review the messages. If you are interested in a particular message, select the message to open it. This will open a pane on the right side of the screen that displays the details associated with that message. When you are finished reviewing the message, select the X in the upper right corner of the pane to close it. Review as many messages as you would like.
15. Leave your Edge browser open as well as the Microsoft Office Home tab and the Microsoft 365 admin center tab. All remaining tasks in this exercise will use LON-CL1 and the Microsoft 365 admin center.

4.3.2 Task 2 - Explore the Exchange admin center

1. After completing the prior task, you should still be in **LON-CL1** and logged into the **Microsoft 365 admin center**. In the left-hand navigation pane, under the **Admin centers** group, select **Exchange**. A new tab will open displaying the **Exchange admin center**.
2. In the **Exchange admin center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.
3. When you have finished exploring the Exchange admin center, close its tab in the Edge browser (leave all other tabs open).

4.3.3 Task 3 - Explore the Teams admin center

1. After completing the prior task, you should still be in **LON-CL1** and logged into the **Microsoft 365 admin center**. In the left-hand navigation pane, under the **Admin centers** group, select **Teams**. A new tab will open displaying the **Teams admin center**.
2. In the **Teams admin center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.
3. When you have finished exploring the Teams admin center, close its tab in the Edge browser (leave all other tabs open).

4.3.4 Task 4 - Explore the SharePoint admin center

1. After completing the prior task, you should still be in **LON-CL1** and logged into the **Microsoft 365 admin center**. In the left-hand navigation pane, under the **Admin centers** group, select **SharePoint**. A new tab will open displaying the **SharePoint admin center**.
2. In the **SharePoint admin center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.
3. When you have finished exploring the SharePoint admin center, close its tab in the Edge browser (leave all other tabs open).

4.3.5 Task 5 - Explore the Microsoft 365 Security admin center

1. After completing the prior task, you should still be in **LON-CL1** and logged into the **Microsoft 365 admin center**. In the left-hand navigation pane, under the **Admin centers** group, select **Security**. A new tab will open displaying the **Security & Compliance admin center**.
2. In the **Security & Compliance admin center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.
3. In the **Security & Compliance admin center**, note the banner at the top of the page that indicates Microsoft 365 Security and Compliance functionality has been split into separate admin centers - a Microsoft 365 Security center and a Microsoft 365 Compliance center.

   In the banner, select the link to the **Microsoft 365 security center**.
4. In the **Microsoft 365 Security center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.
5. When you have finished exploring the Microsoft 365 Security center, close its tab in the Edge browser (leave all other tabs open).

4.3.6 Task 6 - Explore the Microsoft 365 Compliance admin center

1. After completing the prior task, you should still be in **LON-CL1** and logged into the **Microsoft 365 admin center**. In the left-hand navigation pane, under the **Admin centers** group, select **Compliance**. A new tab will open displaying the **Microsoft 365 Compliance center**.

2. In the **Microsoft 365 Compliance center**, take turns selecting each of the items in the left-hand navigation pane. Review the information that is displayed for each item. Navigate through the available tabs that are displayed at the top of the page for each item.

   Note: If you will recall, in the prior task when you selected **Security**, the **Security and Compliance Center** displayed a banner indicating that security and compliance had been split apart. If you had selected the link in the banner to the **Microsoft 365 Compliance center**, it would have displayed this same **Microsoft 365 Compliance center** that you navigated to from the Microsoft 365 admin center.

3. When you have finished exploring the Microsoft 365 Compliance center, close its tab in the Edge browser (leave all other tabs open).

4. At this point, you should just have the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab open in your Edge browser. Leave these tabs open in the browser as they will be used in the next lab.

5 End of Lab 1

6 Module 2 - Lab 2 - Exercise 1 - Managing Microsoft 365 users with the Microsoft 365 admin center

Holly Dickson is Adatum's Enterprise Administrator. Since she doesn't have a personal Microsoft 365 user account set up for herself, Holly initially signed into Microsoft 365 as the default Microsoft 365 MOD Administrator account. In this task, she will create a Microsoft 365 user account for herself, and she will assign her user account the Microsoft 365 Global Administrator role, which gives her the ability to perform all administrative functions within Microsoft 365.

In your role as Holly Dickson, you will then create several additional user accounts in the Microsoft 365 admin center, each of which you will later add to new security groups that you'll also create. While Enterprise Admins typically do not add user accounts, this is a one-time task that you need to perform to prepare Adatum's test environment for future lab exercises in this course.

Important: As a best practice in your real-world deployments, you should always write down the first global admin account's credentials (in this lab, the MOD Administrator) and store it away for security reasons. This account is a non-personalized identity that owns the highest privileges possible in a tenant. It is **not** MFA activated (because it is not personalized) and the password for this account is typically shared among several users. Therefore, this first global admin is a perfect target for attacks, so it's always recommended to create personalized service admins and keep as few global admins as possible. For those global admins that you do create, they should each be mapped to a single identity (just as you're doing in this task for Holly), and they should each have MFA enforced. For the purpose of this lab environment, you will turn on MFA for Holly in the next lab exercise, which focuses on setting password policies.

6.0.1 Task 1 - Create Microsoft 365 users

In this task, you will take on the persona of Holly Dickson, Adatum's Microsoft 365 Enterprise Administrator. Now that she has provisioned Adatum's Microsoft 365 tenant in the prior lab, Holly is ready to begin adding user accounts for her pilot project. She will begin by adding a personalized account for herself, and then she will add user accounts for additional users who will be part of the pilot.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior lab. The **Microsoft 365 admin center** should still be open in the Edge browser, and you should be signed into Microsoft 365 as the **MOD Administrator**.

2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then select **Active users**.

   In the **Active users** list, you will see the list of existing user accounts that were created for Adatum by your lab hosting provider. Since you're taking on the role of Holly Dickson in this lab scenario, you will create a user account for yourself, and you will assign yourself the Microsoft 365 role of Global Administrator, which gives Holly global access to all management features and data across Microsoft online services.

3. In the **Active Users** window, select **Add a user** then **Single user** that appears on the menu bar above the list of active users.

4. In the **Set up the basics** window, enter the following information:

- First name: **Holly**
- Last name: **Dickson**
- Display name: When you tab into this field, **Holly Dickson** will appear.
- Username: **Holly**

  IMPORTANT: To the right of the **Username** field is the domain field. It will be prefilled with whatever domain is identified as the **Default domain** for the organization. For Adatum, this will be the **xxxUPNxxx.xxxCustomDomainxxx.xx** domain that was created for this MS-030 lab environment by your lab hosting provider and which you finished provisioning in Lab 1.

  However, for the purposes of future lab exercises concerining directory synchronization, you should set the domain for each new user that you create in this task to the original **M365xZZZZZZ.onmicrosoft.com** cloud domain (where ZZZZZZ is your tenant ID provided by your lab hosting provider).

  Therefore, you must select the drop-down arrow in this domain field and select **M365xZZZZZZ.onmicrosoft.com**

  After configuring this field, Holly's username should appear as:

  Holly@M365xZZZZZZ.onmicrosoft.com
- Password settings: uncheck **Automatically create a password** option
- Password: **Pa55w.rd**
- Uncheck the **Require this user to change their password when they first sign in** checkbox

5. Select **Next**.
6. In the **Assign product licenses** window, enter the following information:
   - Select location: **United States**
   - Licenses: Verify the **Assign user a product license** option is selected and then select the **Enterprise Mobility + Security E5** check box and the **Office 365 E5** check box
7. Select **Next.**
8. In the **Optional settings** window, select the drop-down arrow to the right of **Roles (User: no administration access).**
9. In the **Roles** information that appears, select the **Admin center access** option. This displays a list of the most commonly assigned administrator roles.
10. If the role you are assigning is not in this list, then you can select the **Show all by category** drop-down arrow to display all the available roles (sorted by category). However, in this case, Holly wants to assign herself the Global Administrator role. She can do this since she is logged in as the MOD Administrator, which is also a Global admin. Only a Global admin can assign another user the Global admin role.

    Select **Global Admin** and then select **Next**.
11. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.
12. On the **Holly Dickson added to active users** page, as a final verification, select **Show** that appears next to the **Password** to verify you entered **Pa55w.rd** correctly. Select **Close**.
13. Repeat steps 3-12 to add the following users and data:

    Username domain: When you enter the **Username** for each of these users, make sure that you select the **M365xZZZZZZ.onmicrosoft.com** domain in the domain field, just as you did when you created Holly's username.

    Password: Assign each user the **Pa55w.rd** password, and just like with Holly's account, do NOT require they change the password at their first login.

    Licenses: Assign **Alan Yoo** the **Office 365 E5** license. For all other users, select the **Create user without product license (not recommended)** option.

Roles: By default, a user is assigned the **User role (no administration access)**; this will be sufficient for these users for now. In Lab 2, Exercise 5, you will assign roles to the users. So when you reach the **Optional settings** window, select **Next** to bypass assigning a role.

- **Alan Yoo** with username **Alan**; assign an **Office 365 E5** license but no role
- **Ada Russell** with username **Ada**; do not assign a license or role
- **Adam Hobbs** with username **Adam**; do not assign a license or role
- **Libby Hayward** with username **Libby**; do not assign a license or role
- **Laura Atkins** with username **Laura**; do not assign a license or role

14. Review the list of **Active users**. Verify that each user you added has **M365xZZZZZZ.onmicrosoft.com** as the domain portion of their username.

    If any of the users has **xxxUPNxxx.xxxCustomDomainxxx.xx** as the domain portion of their username, select the user's **Display name** (so that the check mark appears to the left of the **Display name**), select the **ellipsis** icon on the menu bar above the list of users, and in the drop-down menu, select **Edit username**. Then in the **Manage username** window, select the **M365xZZZZZZ.onmicrosoft.com** domain and then select **Save changes**.

15. Remain logged into LON-CL1 with the Microsoft 365 admin center open in your browser for the next task.

6.0.2 Task 2 - Edit Microsoft 365 users

In this task, you will perform a number of the more common editing features applied towards user accounts. You will begin by updating Alan Yoo's contact information, and then you will block him from being able to sign in.

Blocking a user from signing in is a best practice when you feel the user's password or username have been compromised. This prevents the user from signing in and it automatically signs them out from all Microsoft services within 60 minutes.

You will then assign a product license to Ada Russell's account. Finally, you will delete Libby Hayward's account, and then you will restore it.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior task. The **Microsoft 365 admin center** should still be open in the Edge browser, and you should be signed into Microsoft 365 as the **MOD Administrator**.
2. In the **Microsoft 365 admin center** tab, the **Active users** list should still be displayed from the prior task. Select **Alan Yoo** so that the check mark appears in the circle to the left of his name.
3. In the menu bar above the list of users, select the **ellipsis** icon (**More actions**). In the drop-down menu that appears, select **Manage contact information**.
4. In the **Manage contact information** pane that appears for Alan Yoo, enter **Accounts Receivable** in the **Department** field and then select **Save changes**. This will save the information and display a **Contact information updated** message at the top of the pane. Select the X in the upper right corner to close the **Manage contact information** pane.
5. Alan Yoo's account should still be selected in the **Active Users** list. In the menu bar above the list of users, select the **ellipsis** icon again, and this time select **Edit sign-in status** in the drop-down menu.
6. In the **Block sign-in** pane, select the **Block this user from signing in** check box and then select **Save changes**. Note the message that appears at the top of the pane indicating that Alan is now blocked from signing in, and that he will automatically be signed out of all Microsoft services within 60 minutes. Select the X in the upper right corner to close the **Block sign-in** pane.
7. In the **Active users** list, select **Alan Yoo** to unselect his account, and then select **Ada Russell**.
8. For Ada, you want to learn how to assign a new license to an existing user. In the menu bar above the list of users, select **Manage product licenses**.
9. In the **Ada Russell** pane, the **Licenses and Apps** tab is displayed by default (since you selected the **Manage product licenses** option). Under the list of licenses, select the **Office 365 E5** license and then select **Save changes**. Note the message that appears at the top of the pane indicating the delayed

availability for setting Ada up into Microsoft Teams. Select the X in the upper right corner to close the **Ada Russell** pane.

10. In the **Active users** list, not that **Ada Russell** is now assigned an Office 365 E5 license. Select **Ada Russell** to unselect her account, and then select **Libby Hayward**.
11. To the right of Libby Hayward's **Display Name**, select the vertical ellipsis icon. In the drop-down menu that appears, note the options that are available are similar to the options from the ellipsis icon that you select in the menu bar for Alan and Ada, although there are less options to choose from. However, this menu has less choices.
12. In this task, you are going to practice deleting Libby's account and then restore it. You can delete a user by selecting the **Delete user** option on the menu bar, or this option from the vertical ellipsis icon. Since you have selected the vertical ellipsis icon, select **Delete user** from the drop-down menu.
13. On the **Delete this user?** pane, select the **Delete user** button that appears at the bottom of the pane.
14. On the **Libby Hayward has been deleted** pane, select the **Close** button.
15. Select the **Refresh** icon at the top of the browser (to the left of the address bar). Verify that **Libby Hayward** no longer appears in the list of **Active users**.
16. Now verify that Libby appears in the list of deleted users. In the **Microsoft 365 admin center**, in the left-hand navigation pane under **Users**, select **Deleted users**.
17. In the **Deleted users** page, verify that **Libby Hayward** appears in the list of deleted users.
18. Deleting a user performs a soft-delete on the account; this allows organizations to restore deleted users for up to 30 days following their deletion. You should now restore Libby's account to an active user. In the **Deleted users** list, select **Libby Hayward**.
19. On the menu bar, select **Restore user**.
20. In the **Restore Libby Hayward** pane, you have the option of assigning Libby a new password yourself or auto-generating a new password. **A good practice is to auto generate the password and then make the restored user change their password upon first sign in.**

    Since the **Auto-generate password** option is selected by default as well as the **Make this user change their password when they first sign in** option, simply select the **Restore** button at the bottom of the pane.
21. In the **Libby Hayward has been restored** window, it confirms that Libby's account has been restored and that her password has been reset. You also have the option to send the password to Libby in an email.

    Select the **Send password in email** check box, and then in the **Email the new password to the following recipients** field, it displays the MOD Administrator's email. After this email address, enter a semicolon followed by Libby's email of **libby@M365xZZZZZZ.onmicrosoft.com** (replace ZZZZZZ with the tenant ID). When you have finished entering Libby's email, select the **Send email and close** button.
22. Libby's account should no longer appear in the **Deleted users** list. In the **Microsoft 365 admin center**, in the left navigation pane, select **Active users**.
23. Verify that **Libby Hayward** appears in the list.
24. Leave the Edge browser session open as well as all the browser tabs.

6.0.3 Task 3 - Verifying user settings

In this task, you will verify several of the changes you made to user accounts in the prior task. You will sign into Microsoft 365 as Libby Hayward, which will require that you enter the new temporary password assigned to her account. You will then attempt to sign into Microsoft 365 as Alan Yoo, and you will validate whether his blocked account can sign in.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior task. The **Microsoft 365 admin center** should still be open in the Edge browser, and you should be signed into Microsoft 365 as the **MOD Administrator**.

2. You must now retrieve the temporary password that was assigned to Libby Hayward's account when you restored her account in the prior task. At the time you restored her account, you selected the option to send an email to Libby's mailbox as well as the MOD Administrator's mailbox that contained the temporary password.

   In this task, you will sign into the MOD Administrator's Outlook mailbox and retrieve the temporary password. You will then switch to a new client machine and attempt to log into Microsoft 365 as Libby using the new password. Since you also selected the option that forces Libby to create a new password at her first log in, you will have to change the password at that time.

   In your web browser, select the **Microsoft Office Home** tab. In the **Microsoft Office Home** page, select the **Outlook** icon. This will open Outlook for the MOD Administrator's mailbox.

3. In the **Welcome** window that appears for Outlook, select the X in the upper right-hand corner to close it.

4. In the MOD Administrator's **Inbox** in Outlook, select the email message in which the **From** account is **Microsoft on behalf of your organization** and the Subject line is **Account information for new or modified users**.

   This email should display the temporary password that was assigned to Libby Hayward's account at the time her deleted account was restored. Write down the temporary password.

5. You must now log out of Microsoft 365 as the MOD Administrator and log back in as Libby Hayward. To log out of the MOD Administrator account, select the circle in the upper right portion of the Edge browser that contains the **MA** initials. In the drop-down menu that appears, select **Sign out**.

6. Once the dialog box appears indicating your are signed out of your account, it is a best practice to close all other tabs the MOD Administrator had open. This eliminates the chance that you will select a tab for the old account (MOD Administrator) when you sign in as a new account (Libby Hayward).

   Therefore, close the **Microsoft Office Home** tab, the **Microsoft 365 admin center** tab, and any other tab that is open. Only the **Sign out** tab should remain open.

7. In the **Sign out** tab, enter the following URL in the address bar: **https://portal.office.com**

8. In the **Pick and account** dialog box, select **Use another account**.

9. In the **Sign in** window, enter **Libby@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ should be replace with your tenant ID). Select **Next**.

10. In the **Enter password** window, enter the temporary password that was assigned to Libby's restored user account and then select **Sign in**.

11. In the **Update your password** dialog box, enter Libby's temporary password in the **Current password** field, and then enter **Pa55w.rd** in the **New password** and **Confirm password** fields. Select **Sign in**.

12. If you receive an error message indicating the new password has been entered too many times before, enter **Ynot-Knirf@0827** in the **New password** and **Confirm password** fields and then select **Sign in**.

13. Verify that you can access the Office 365 Home page. Note that no Office 365 applications appear on the home page; this is because Libby was never assigned a Microsoft 365 license.

14. You must now log out of Microsoft 365 as Libby Hayward and then log back in as Alan Yoo. To log out of the Libby Hayward account, select the circle in the upper right portion of the Edge browser that contains the **LH** initials. In the drop-down menu that appears, select **Sign out**.

15. Once you are signed out, enter the following URL in the address bar: **https://portal.office.com**

16. In the **Pick and account** dialog box, select **Use another account**.

17. In the **Sign in** window, enter **Alan@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ should be replace with your tenant ID). Select **Next**.

18. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.

19. In the **Pick and account** dialog box, note the error message that indicates Alan's account has been blocked. You have verified that Alan cannot log into Microsoft 365.

20. You will now log back into Microsoft 365 as Holly Dickson using the personal account that she previously set up for herself. In the **Pick and account** dialog box, select **Use another account**.

21. In the **Sign in** window, enter **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ should be replace with your tenant ID). Select **Next**.
22. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
23. If a **Get your work done with Office 365** dialog box appears, select the X in the upper right corner to close it.
24. In the **Office 365 Home** page, select **Admin**.
25. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then select **Active users**.
26. In the **Active users** list, select **Alan Yoo**.
27. In the menu bar that appears above the list of users, select the **ellipsis** (**More actions**) icon, and then in the drop-down menu that appears, select **Edit sign-in status**.
28. On the **Unblock sign-in** pane, the **Block this user from signing in** check box is selected. Select this check box to clear it and then select **Save changes**.
29. Once a message appears at the top of the pane indicating that Alan Yoo is now unblocked from signing in, select the X in the upper right corner of the **Unblock sign in** pane to close it. Note the message that it may take up to 15 minutes before Alan can sign in again.
30. Remain signed into Microsoft 365 on LON-CL1 as Holly Dickson, and leave your browser and all tabs open for the next lab exercise.

Results: After completing this exercise, you should have created and managed user accounts and licenses according to Adatum's business needs.

7 Proceed to Lab 2 - Exercise 2

8 Module 2 - Lab 2 - Exercise 2 - Managing Microsoft 365 password policies

In this exercise, you will continue in your role as Holly Dickson, Adatum's Enterprise Administrator. As part of Adatum's Microsoft 365 pilot project, Holly wants to explore Microsoft 365 password management functionality. She will begin by configuring a Microsoft 365 password policy that sets user passwords to expire after 90 days and receive an upcoming expiration notification 14 days prior to expiration.

Since Adatum is also interested in implementing Multi-factor authentication (MFA), Holly has been tasked with introducing MFA in their pilot project. MFA is a security standard that provides a stepping stone for businesses to strengthen user integrity. Multi-factor authentication is turned On by default for a Microsoft 365 tenant; however, for the purposes of this lab, MFA has been turned Off to enable Microsoft 365 to function more efficiently in your virtual lab environment. Therefore, Holly will turn on MFA for her own personal account to verify its functionality, and then she will turn it back off. At the end of this exercise, you will disable MFA for Holly's account. This will save you from having to enter the second form of authentication when signing in as Holly in any of the remaining labs in this course.

Important: To implement MFA, you will need to use your mobile phone to receive a verification code so that you can enter it into your tenant as a second form of authentication. If you do not have a phone, you will have to skip this lab. If this is the case, notify your instructor, who can potentially partner you with another student to follow along through this lab.

8.0.1 Task 1 - Configure the Microsoft 365 password policy

In this task, you will change Adatum's password policy that controls how often users must change their password. A good practice is to have your users change their passwords every 90 days with a warning of 14 days prior to the update, both of which are the default settings in Microsoft 365. However, for this lab exercise, you will change password expiration to occur every 14 days, with a 14 day notification.

Important - You are making this change simply for testing purposes. Since all users' passwords will expire within 14 days, and with a notification window of 14 days, they will all be within the 14 day notification window. This will enable you to see what happens when a user falls within the 14 day window prior to his or her password

expiring. In this task you will make this policy change; in the next task, you will test the ramifications of this change.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior lab exercise. The **Microsoft 365 admin center** should still be open in the Edge browser, and you should be signed into Microsoft 365 as **Holly Dickson**.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Settings** and then select **Org settings**.
3. In the **Org settings** window, the **Services** tab is displayed by default at the top of the page. Select the **Security & Privacy** tab located next to it.
4. In the **Security & Privacy** page, select the **Password expiration policy** in the list of settings.
5. In the **Password expiration policy** pane that appears, select the check box for **Set user passwords to expire after a number of days**.
6. Enter **14** in the **Days before passwords expire** field. Leave the **Days before a user is notified about expiration** field set to 14. Select **Save changes**.
7. Verify that the **Changes saved** message appears at the top of the page and then select the X in the upper right corner of the pane to close it.
8. Leave your browser and all its tabs open for the next task.

8.0.2 Task 2: Validate the password policy

In this task, you will validate the change that you made in the prior task when you set the password expiration setting to 14 days. With a 14 day notification window, you should now be able to see what happens when a user's password is due to expire and you are within the notification window.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior lab exercise.
2. To see the affect of the password policy change, first sign out of Microsoft 365 as Holly Dickson. On the **Microsoft 365 admin center** tab, select the **HD** icon in the upper right corner of the screen, and in the window that appears, select **Sign out**.
3. Close your **Edge** browser and all the tabs to clear your cache. Once the browser is closed, select the **Edge** browser icon on the taskbar to re-open it.
4. In the Edge browser, enter the following URL in the address bar: **https://portal.office.com**.
5. In the **Pick an account** window that appears, you want to sign back in as Holly Dickson, so select **holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID).
6. In the **Enter password** window, enter provided by your lab hosting provider and then select **Sign in**.
7. If the **Get your work done with Office 365** window appears, then select the X in the upper right-hand corner of the window to close it.
8. On the upper-right side of the window, verify that a notification appears with the following information: **Time to change your password. Your password will expire in 13 days.**

   Note: It may take a few minutes before the password change notification message appears.
9. Now that you have verified that your revised password policy works since you received a notification message indicating you must change your password, you should reset the policy by setting the expiration days from 14 back to 90.

   Since you just logged into Microsoft 365 as Holly Dickson, in the **Microsoft Office Home** page, select **Admin** to open the **Microsoft 365 admin center**.
10. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all**, then select **Settings**, and then select **Org settings**.
11. In the **Org settings** window, the **Services** tab is displayed by default at the top of the page. Select the **Security & Privacy** tab located next to it.
12. In the **Security & Privacy** page, select the **Password expiration policy** in the list of settings.

13. In the **Password expiration policy** pane that appears, select the check box for **Set user passwords to expire after a number of days**.
14. Enter **90** in the **Days before passwords expire** field. Leave the **Days before a user is notified about expiration** field set to 14. Select **Save changes**.
15. Verify that the **Changes saved** message appears at the top of the page and then select the X in the upper right corner of the pane to close it.
16. Leave your browser and all its tabs open for the next task. While you would normally close your browser and then re-open it to reset the password policy, you don't need to do it here. In the next task, you will enable Multi-factor Authentication, which will require you to close and then re-open your browser. There's no reason to close and re-open your browser now and then do it again in the next task. Simply proceed to the next task.

8.0.3 Task 3 - Enable and Disable Multi-factor authentication

To test Multi-factor authentication (MFA), Holly Dickson wants to turn it on for her personal Microsoft 365 user account and test how it works. Once you have verified that you can connect to Microsoft 365 using MFA, you will disable MFA for Holly's account. This will save you from having to enter the second form of authentication when signing in as Holly in any of the remaining labs in this course.

Important: To implement MFA, you will need a mobile phone to receive a text message containing a verification code. You will then enter the code into the Office 365 sign-in process as a second form of authentication.

If you do not have a mobile phone:

- You can still perform this task, but you will have to skips steps 8-17 that verify MFA by having you log out and then enter a second form of authentication when you log back in to Office 365.
- If you are in a classroom training environment, it is recommended that you notify your instructor, who can then potentially partner you with another student who has a mobile phone so that you can either use the other student's phone or watch the other student sign in.
- If you are performing this training on your own and you do not have a mobile phone, or if you are in a classroom environment but cannot partner with another student, you can perform the steps in this task other than the ones that actually verify MFA (steps 8-17). This still allows you to enable and then disable MFA to get the experience of performing those steps.

This is the only task in this course that requires a mobile phone.

1. You should still be logged into the **LON-CL1** VM as the **Administrator**.
2. The **Microsoft 365 admin center** should still be open in the Edge browser from the prior task, and you should be signed into Microsoft 365 as **Holly Dickson**.
3. To enable MFA for Holly Dickson's user account, you must first access the **Active users** list in the **Microsoft 365 admin center**. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then select **Active users**.
4. In the **Active users** window, on the menu bar at the top of the user list, select **Multi-factor authentication**. This will open a **multi-factor authentication** window in a new tab in your browser.
5. In the **multi-factor authentication** window, the **users** tab is displayed by default. Note the MFA status for all existing user accounts is **Disabled**.

   Select the check box for **Holly Dickson**, and in Holly's properties pane that appears on the right, select **Enable**.
6. On the **About enabling multi-factor auth** dialog box, select **enable multi-factor auth**.
7. When the **Updates successful** dialog box appears, select **close**. In the list of users in the **multi-factor authentication** window, verify Holly's MFA Status has changed to **Enabled**.
8. You must now sign out of Microsoft 365 as Holly, close your browser session (to clear cache), open a new session, and then log back into Microsoft 365 as Holly. During the log-in process, you will be required to enter a second form of authentication as per MFA. When Holly signs back in after having MFA enabled for her user account, she will be asked for the authentication information needed for MFA, such as her phone number and authentication options. In your role as Holly, you will enter your mobile phone number, and you will receive a text message containing a verification code that you must enter to validate the authentication. You will perform these steps in the remaining portion of this task.

You must begin by signing out of Microsoft 365 as Holly, so select the **HD** user icon in the upper right corner of the browser (on the **multi-factor authenication** window, it may display Holly's username instead of her initials) and in the **My account** pane, select **Sign out**.

9. Once you are signed out, close the browser and all the browser tabs.
10. Select the **Edge** icon on your taskbar to open a new browser session, and then open the **Office 365 Home** page by entering the following URL in the address bar: **https://portal.office.com**
11. In the **Pick an Account** window, select **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant suffix ID provided by your lab hosting provider). In the **Enter password** window, enter **Pa55w.rd** and select **Sign in**.
12. Because MFA is enabled for Holly, a **More information required** window appears. Select **Next**.
13. In the **Keep your account secure** window, it indicates that you can either use the Microsoft Authenticator app for MFA, or you can use a phone.

    For the purposes of this lab, you should use the **Phone** method so that you do not have to take time installing the Microsoft Authenticator app that you may not use again after this training class. Since the window displays the Microsoft Authenticator method by default, select the **I want to set up a different method** option at the bottom of the window.
14. In the **Choose a different method** dialog box that appears, select the drop-down arrow in the **Which method would you like to use** field and select **Phone**. Select **Confirm**.
15. In the **Keep your account secure** window, the **Microsoft Authenticator** section has now been replaced by a **Phone** section. Select your country or region from the drop-down list, enter your mobile phone number (**xxx-xxx-xxxx**), and then select **Next**.

    Note: If you receive a message indicating that an error occurred, you should close the browser (closing all tabs) and then repeat steps 10-15.
16. You will receive a text message on your mobile phone with a verification code to test whether the phone number you entered is correct. In the **Enter code** window that appears, enter the code that was sent in the text message and then select **Verify**.

    Note: If you take too long to complete this process, the **Enter password** window will appear with a message indicating you took too long to complete the sign in process, so you will be timed-out. If this occurs, you must sign in again with Holly's password of **Pa55w.rd**. Another verification code will be texted to your phone, so enter it in the **Enter code** screen that appears and select **Verify**.
17. If a **Stay signed in?** window appears, select **Don't show this again** and then select **Yes**.
18. The **Office 365 Home** page should now be displayed in your browser. While Adatum will institute MFA once it eventually goes live with Microsoft 365 in its production environment, for now Holly wants to turn MFA off for her account for the remainder of the pilot project. She has just verified that she can use MFA to sign into Microsoft 365, so she will turn it off through the remainder of the pilot.

    To disable MFA for Holly Dickson's user account, select **Admin** on the **Office 365 home** page to open the **Microsoft 365 admin center**. In the left-hand navigation pane, select **Users** and then **Active users**.
19. In the **Active users** window, on the menu bar at the top of the user list, select **Multi-factor authentication**.
20. In the **multi-factor authentication** window, the **users** tab is displayed by default. Note the MFA status for all existing user accounts is **Disabled**, except for Holly's account, which displays a status of **Enforced**.

    Note: When you originally enabled MFA for Holly, the status was changed from **Disabled** to **Enabled**. However, now that Holly has signed in using MFA, her the status has changed from **Enabled** to **Enforced**.

    Select the check box for **Holly Dickson**, and in Holly's properties pane on the right, select **Disable**.
21. On the **Disable multi-factor authentication?** dialog box, select **yes**.
22. When the **Updates successful** dialog box appears, select **close**. In the **multi-factor authentication** window, verify Holly's MFA Status has changed to **Disabled**.

23. You must now sign out of Microsoft 365 as Holly, close your browser session (to clear your cache), open a new session, and then log back into the **Office 365 home** page as Holly (**Holly@M365xZZZZZZ.onmicrosoft.com**). You should be familiar with these processes, so perform them now.

    Note: with MFA turned off for Holly's account, you will simply need to enter Holly's password of **Pa55w.rd** when she logs in. Once you are logged in, you should then navigate to the **Microsoft 365 admin center**.

24. After having completed the prior step, you should be logged into Microsoft 365 as Holly, and you should have the **Microsoft Office Home** page and the **Microsoft 365 admin center** open in your browser. Leave the browser and these tabs open and proceed to the next lab exercise.

Results: After completing this exercise, you should have configured and validated an Microsoft 365 password policy, including MFA.

9 Proceed to Lab 2 - Exercise 3

10 Module 2 - Lab 2 - Exercise 3 - Managing Microsoft 365 groups

Earlier in this lab, you added several new Microsoft 365 user accounts. As you continue in your role as Holly Dickson, Adatum's Enterprise Admin, you now want to investigate implementing Microsoft 365 groups. In this exercise, you will create two new Microsoft 365 groups and then manage the groups by assigning users to them. You will also analyze the effect on group members when you delete a group.

10.0.1 Task 1: Creating Microsoft 365 groups

In your role as Holly Dickson, you now want to implement Microsoft 365 groups as part of your pilot project. In this task, you will add two Sales-related groups and a group for Accounts Receivable users. You will then delete one of the Sales groups and verify that deleting a group does not delete the user accounts that were members of the group.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.
2. The **Microsoft 365 admin center** should still be open in the Edge browser from the prior exercise, and you should be signed into Microsoft 365 as **Holly Dickson** (Holly@M365xZZZZZZ.onmicrosoft.com). In the **Microsoft 365 admin center**, select **Groups** in the navigation pane on the left, and then under it, select **Active Groups**.
3. In the **Active Groups** window, select **Add a group** on the menu bar at the top of the page.
4. In the **Choose a group type** pane that appears, the **Microsoft 365** group type is selected by default. Accept this value by selecting **Next**.
5. In the **Set up the basics** window, enter **Inside Sales** in the **Name** field and **Collaboration group for the Inside Sales team** in the **Description field** and then select **Next** (Note - if you leave the **Description** field blank, you must still select it to enable the **Next** button).
6. In the **Assign owners** window, select the **Owners** field, which displays the list of active users. Select **Alan Yoo** and then select **Next**.
7. In the **Edit settings** window, enter **insidesales** in the **Group email address** field.

```
**Note:** To the right of the **Group email address** field is the domain field. It's already pre

After configuring this field, the Inside Sales group email address should appear as: **insidesale

After configuring the email address, under the **Privacy** section, leave the default setting of
```

8. On the **Review and finish adding group** window, review the information and if anything needs to be changed, select the appropriate **Edit** option; otherwise, select the **Create group** button at the bottom of the page.
9. On the **New group created** window, note the message that appears at the top of the page that indicates it may take up to 5 minutes before the group appears in the list of active groups.

Since you will adding additional groups, under the **Next step** section towards the bottom of the page select **Add another group**. If you already closed this window, then from the **Active groups** page, select **Add a group**.

10. Repeat steps 4-9 to add another group with the following information (this time select **Close** once the group is added and not the **Add another group** option):
    - Type: **Security**
    - Name: **Sales**
    - Description: **Sales Department users**

    Note: There is no owner, email address, or privacy setting for Security groups
11. In the **Active groups** window, if both new groups do not appear in the list, select **Refresh** on the menu bar above the list. Both groups should now appear (you may have to wait a few minutes and then Refresh again).
12. You're now ready to add members to the groups. In the list of **Active groups**, select the **Inside Sales** group, which opens a window for the group.
13. In the **Inside Sales** window, the **General** tab is displayed by default. Select the **Members** tab.
14. In the **Members** tab, you can see that there are zero (0) members. Select **View all and manage members** to add members to the group.
15. In the **Inside Sales** group window, select **+Add members**. This displays the list of current users.
16. In the list of users, select **Ada Russell** and **Alan Yoo** and then select **Save**.
17. Select **Close**. This displays the list of users for this group. Select **Close** again.
18. On the **Inside Sales** window, select the **X** in the upper right-hand corner to close the window.
19. In the **Active groups** window, select **Add a group** on the menu bar and then add a new group with the following information:
    - Type: **Security**
    - Name: **Accounts Receivable**
    - Description: **Accounts Receivable department users**
20. If the Accounts Receivable group does not appear in the **Active groups** list, select **Refresh** on the menu bar (you may need to wait a few minutes and then Refresh again). The group should now appear.
21. In the **Active groups** list, select the **Accounts Receivable** group, which opens a window for the group.
22. In the **Accounts Receivable** group window, select the **Members** tab.
23. In the **Members** tab, you can see that there are zero (0) group owners and members. Select **View all and manage owners** to add an owner for the group.
24. In the **Accounts Receivable** group window, select **+Add owners**. This displays the list of current users.
25. In the list of users, select **Libby Hayward** and then select **Save**.
26. Select **Close**. This displays the list of owners for this group. Select **Close** again.
27. In the **Members** tab of the **Accounts Receivable** window, select **View all and manage members** to add members to the group.
28. In the **Accounts Receivable** window, select **+Add members**. This displays the list of current users.
29. In the list of users, select **Adam Hobbs** and **Libby Hayward** and then select **Save**.
30. Select **Close**. This displays the list of users for this group. Select **Close** again.
31. On the **Accounts Receivable** window, select the X in the upper right-hand corner to close the window. This will return you to the list of **Active groups**.
32. You now want to test the effect of deleting a group. In the list of **Active groups,** select the vertical ellipsis icon (**More actions**) to the right of the **Inside Sales** group. In the menu box, select **Delete group**.

33. In the **Delete Inside Sales?** window, select the **Delete group** button.
34. On the **Inside Sales was deleted** window, select **Close**.
35. This will return you to the list of **Active groups** in the **Microsoft 365 admin center**. The **Inside Sales** group should no longer appear.
36. To verify whether deleting this group affected any of its members, in the left-hand navigation pane of the **Microsoft 365 admin center**, select **Users** and then **Active Users**.
37. In the list of **Active Users** verify that the two members of this group, **Ada Russell** and **Alan Yoo**, still appear in the list of users. This verifies that deleting a group does not delete the user accounts that were members of the group.
38. Leave your browser and all tabs open and proceed to the next lab exercise.

Results: After completing this exercise, you should have created and managed Microsoft 365 groups and security groups.

11 Module 2 - Lab 2 - Exercise 4 - Managing Microsoft 365 users and groups with Windows PowerShell

Windows Powershell can improve the way an administrator can automate and streamline complicated or simple tasks that can be time-consuming when performed in the Microsoft 365 user interface. By entering commands directly to the tenant, tasks that would take hours by hand can be reduced to minutes or even seconds with PowerShell.

In this exercise, you will continue in your role as Holly Dickson. Holly wants to perform some basic user maintenance using Windows PowerShell. This will enable her to compare her experience creating and maintaining users in the Microsoft 365 admin center to performing the same tasks using Windows PowerShell.

To implement PowerShell in a Microsoft 365 deployment, you must first install the Microsoft Online Services Sign-In Assistant, which provides end user sign-in capabilities to Microsoft Online Services, such as Microsoft 365. This assistant installs client components that allow common applications, such as Microsoft Outlook, to authenticate to Microsoft Online Services. The Microsoft Online Services Sign-In Assistant can also provide an improved sign-in experience, such that end users can access Microsoft Online Services without having to re-enter their credentials (such as a user name or password).

Once the Microsoft Online Services Sign-In Assistant is installed, you will use Windows PowerShell to create new user accounts and assign them licenses, modify existing user accounts, create Microsoft 365 groups using, and configure user passwords.

11.0.1 Task 1 - Installing Microsoft Azure Active Directory module for Windows PowerShell

In this task you are going to lay the foundation for editing and managing the Microsoft 365 tenant with the use of PowerShell. The next step is to install the Microsoft Online Services Sign-In Assistant, which provides end user sign-in capabilities to Microsoft Online Services, such as Microsoft 365.

The Microsoft Online Services Sign-In Assistant installs client components that allow common applications, such as Microsoft Outlook, to authenticate to Microsoft Online Services. The Microsoft Online Services Sign-In Assistant can also provide an improved sign-in experience, such that end users can access Microsoft Online Services without having to re-enter their credentials (such as a user name or password). This download is intended for IT professionals for distribution to managed client systems as part of a Microsoft 365 client deployment through System Center Configuration Manager (SCCM) or similar software distribution systems.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.
2. Your **Edge** browser should still be open from the prior lab exercise. You should be logged into Microsoft 365 as Holly Dickson, and the browser should have tabs open for the **Microsoft Office Home** page and the **Microsoft 365 admin center**.

   Open a new tab in your browser and then enter the following URL in the address bar: **http://aka.ms/t01i1o**
3. This will take you to the **Microsoft Download Center** for the **Microsoft Online Services Sign-In Assistant for IT Professionals RTW**. Select the **Download** button.

4. On the **Choose the download you want** page, select the **msoidcli_64.msi** check box and then Select **Next**.
5. In the notification bar that appears at the bottom of the page, once the **msoidcli_64.msi** file is saved, select **Open file**.
6. On the **Do you want to run this file?** dialog box, select **Run**.
7. In the **Microsoft Online Services Sign-in Assistant Setup** wizard, select **I accept the terms in the License Agreement and Privacy Statement**, and then Select **Install**.
8. If a **Do you want to allow this app to make changes to your device** dialog box appears, select **Yes**.
9. On the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, select **Finish**.
10. Close the tab in your Edge browser for the **Download Center**.
11. In the Search box in the bottom left corner of your taskbar, enter **powershell**.
12. In the list of search results, right-click on **Windows PowerShell**, and in the menu that appears select **Run as administrator**.
13. If a **Do you want to allow this app to make changes to your device** dialog box appears, select **Yes**.
14. Maximize your PowerShell window. In **Windows PowerShell**, at the command prompt type the following command and then press Enter:

    ```
    Install-Module MSOnline
    ```

15. If you are prompted to install the **NuGet provider**, enter **Y** to select [**Y**] **Yes**.
16. If you are prompted to confirm whether you want to install the module from an untrusted repository (PSGallery), enter **A** to select [**A**] **Yes to All.**
17. Once the installation is complete, the screen will return to the Windows PowerShell command prompt. At the command prompt type the following command to install the Azure AD PowerShell module that you just retrieved in the earlier step and then press Enter:

    ```
    Install-Module AzureADPreview
    ```

18. If you are prompted to confirm whether you want to install the module from an untrusted repository (PSGallery), enter **A** to select [**A**] **Yes to All.**
19. Once the installation is complete, the screen will return to the Windows PowerShell command prompt. You have now installed the **Windows Azure Active Directory PowerShell Module**.
20. Leave the Windows PowerShell window open and proceed to the next task.

11.0.2 Task 2 - Create new users and assign licenses by using Windows PowerShell

In a previous lab exercise, you created new user accounts using the **Microsoft 365 admin center**. In this task, you will create two new users using Windows PowerShell, and you will assign each an **Office 365 E5** license. You will then delete one of the users and then restore the deleted user's account back to the Active users list.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.
2. You should still have the **Windows PowerShell** window open from the prior task. At the command prompt type the following command that connects your PowerShell session to the Microsoft Online Service and then press Enter:

    ```
    Connect-MsolService
    ```

3. In the **Sign in** dialog box that appears, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) with a password of **Pa55w.rd**.

4. PowerShell's execution policy settings dictate what PowerShell scripts can be run on a Windows system. Setting this policy to **Unrestricted** enables Holly to load all configuration files and run all scripts. At the command prompt, type the following command and then press Enter:

   ```
   Set-ExecutionPolicy unrestricted
   ```

   If you are prompted to verify that you want to change the execution policy, enter **A** to select [**A**] **Yes to All.**

5. At the command prompt, type the following command and then press Enter to create a new user named **Catherine Richard** with a password of **Pa55w.rd** and a location set to **CH**. In Catherine's username in the following command, don't forget to replace **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider. Setting the -ForceChangePassword parameter to false means Catherine will not have to change her password when she signs in the first time.

   ```
   New-MsolUser -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com -DisplayName "Catherine Ric
   FirstName "Catherine" -LastName "Richard" -Password 'Pa55w.rd' -ForceChangePassword $false -
   UsageLocation "CH"
   ```

6. At the command prompt, type the following command and then press Enter to create a new user named **Tameka Reed** with a password of **Pa55w.rd** and a location set to **CH**. In Tameka's username in the following command, don't forget to replace **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

   ```
   New-MsolUser -UserPrincipalName tameka@M365xZZZZZZ.onmicrosoft.com -DisplayName "Tameka Reed" -
   FirstName "Tameka" -LastName "Reed" -Password 'Pa55w.rd' -ForceChangePassword $false -
   UsageLocation "CH"
   ```

7. At the command prompt, type the following command and then press Enter to display all the users who are unlicensed:

   ```
   Get-MsolUser -UnlicensedUsersOnly
   ```

8. At the command prompt, type the following command and then press Enter to show all available licenses inside Adatum's Microsoft 365 deployment:

   ```
   Get-MsolAccountSku
   ```

   The ENTERPRISEPREMIUM license is the Office 365 E5 license that was assigned to most of the user accounts. Note that 15 licenses were purchased with Adatum's subscription (Active Units) and 13 have been assigned (Consumed Units). That leaves two licenses available to be assigned.

9. At the command prompt, type the following command and then press Enter to assign a license to **Catherine Richard**. In the command, don't forget to replace the two instances of **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider. This command will assign an Enterprise E5 license to Catherine.

   ```
   Set-MsolUserLicense -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com -AddLicenses "M365xZ
   ```

10. At the command prompt, type the following command and then press Enter to assign a license to **Tameka Reed**. In the command, don't forget to replace the two instances of **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider. This command will assign an Enterprise E5 license to Tameka.

    ```
    Set-MsolUserLicense -UserPrincipalName Tameka@M365xZZZZZZ.onmicrosoft.com -AddLicenses "M365xZZZZZ
    ```

11. At the command prompt, type the following command and then press Enter to block Catherine from signing in. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

    ```
    Set-MsolUser -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com -BlockCredential $true
    ```

12. At the command prompt, type the following command and then press Enter to delete Catherine's user account. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider. Note - This command will delete Catherine's user account without requesting a confirmation.

    ```
    Remove-MsolUser -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com -Force
    ```

13. At the command prompt, type the following command and then press Enter to view the **Deleted Users** list:

```
Get-MsolUser -ReturnDeletedUsers
```

14. Verify that Catherine Richard is in the list of deleted users. Note that it specifies that she is still licensed.
15. At the command prompt, type the following command and then press Enter to restore Catherine's user account to an active user status. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

    ```
    Restore-MsolUser -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com
    ```

16. At the command prompt, type the following command and then press Enter to view the list of deleted users:

    ```
    Get-MsolUser -ReturnDeletedUsers
    ```

17. Since Catherine should have been the only deleted user prior to being restored, there will be no users to display, so PowerShell should simply display the command prompt.
18. At the command prompt, type the following command and then press Enter to view the list of active users:

    ```
    Get-MsolUser
    ```

19. Verify that Catherine Richard is in the active users list.
20. At the command prompt, type the following command and then press Enter to unblock Catherine from signing in to Microsoft 365. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

    ```
    Set-MsolUser -UserPrincipalName Catherine@M365xZZZZZZ.onmicrosoft.com -BlockCredential $false
    ```

21. Leave the Windows PowerShell window open and proceed to the next task.

11.0.3 Task 3 - Bulk Import users using Windows PowerShell

In this task, you will use Windows PowerShell to import a csv file of new user account records into Microsoft 365. The file path is **C:\labfiles\O365Users.csv**.

At first you will attempt to import the users and assign each an **Office 365 E5** license. Based on the outcome of that import, you will make an adjustment to the csv file and re-import the users without a license.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.
2. You should still have the **Windows PowerShell** window open from the prior task.
3. On the taskbar at the bottom of the screen, select the **File Explorer** icon.
4. In **File Explorer** navigate to **C:\labfiles**, right-click on the **O365users.csv** file, and in the menu that appears select **Open with** and then Select **Notepad**.
5. In **Notepad**, review the records for each user account. Note the domain portion of each username is **yourdomain.hostdomain.com**. You need to replace this with **M365xZZZZZZ.onmicrosoft.com** for each user (where you will enter the unique tenant ID provided by your lab hosting provider in place of ZZZZZZ). The easiest way to do this is by doing a Find and Replace. In the menu bar at the top of the **Notepad** window, select **Edit** and then select **Replace**.
6. In the **Replace** window, copy **yourdomain.hostdomain.com** from one of the records and paste it in the **Find what** field, enter **M365xZZZZZZ.onmicrosoft.com** in the **Replace with** field (replacing ZZZZZZ with your tenant ID), and then select **Replace All**.
7. In **Notepad**, review the records for each user account. Note the license assigned to each user is **adatumyyxxxx:ENTERPRISEPACK**. You need to replace this with **M365xZZZZZZ:ENTERPRISEPREMIUM** for each user (where you will enter the unique tenant ID provided by your lab hosting provider in place of ZZZZZZ). The easiest way to do this is by doing a Find and Replace. The **Replace** window should still be open; if you closed it after the prior step, then open it again.
8. In the **Replace** window, copy **adatumyyxxxx:ENTERPRISEPACK** from one of the records and paste it in the **Find what** field, enter **M365xZZZZZZ:ENTERPRISEPREMIUM** in the **Replace with** field (replacing ZZZZZZ with your tenant ID), and then select **Replace All**.
9. Close the **Replace** window.

10. Select the X in the upper right corner of the **Notepad** window to close it. In the **Notepad** dialog box that appears asking if you want to save the changes to the O365Users.csv file, select **Save**.
11. Close File Explorer.
12. In **Windows PowerShell**, copy the following command and paste it in at the command prompt and then press Enter to bulk import the users from the O365Users.csv file into Microsoft 365:

    ```
    Import-Csv -Path C:\labfiles\O365Users.csv | ForEach-Object { New-MsolUser -UserPrincipalName $_."
    ```

13. Notice what happens when you run this command. Each of users in the import file were rejected because Adatum had already consumed all of its Office 365 E5 licenses; therefore, there were no available licenses to assign to these users.

    To work around this for the purposes of your VM lab environment, you will remove the license assignment field from the .csv file. This will add each user and not assign them a license. To do so, open **File Explorer** and then use **Notepad** to open the **O365Users.csv** file.
14. In the **O365Users.csv** file, the first record is the header record. Delete the **LicenseAssignment** field and the comma that follows it.

    Then in each user record, delete the **M365xZZZZZZ:ENTERPRISEPREMIUM** value and the comma that follows it.
15. In **Notepad**, select **File** in the menu bar at the top of the window, and then in the drop-down menu select **Save As**. In the File Explorer window that appears, it's currently pointing to the **C:\Labfiles** folder. In the **File name** field, **O365Users.csv** appears by default. Change the file name to **O365Users_No_Licenses.csv** and then select **Save**.
16. Close **Notepad**.
17. Re-run the Import-Csv command in step 12. However, before you run the command, you must update the command by removing the **-LicenseAssignment $_."LicenseAssignment"** parameter, and you must change the file name to **O365Users_No_Licenses.csv**.
18. Notice what happens when you run this command. Each of users in the import file is successfully added into Microsoft 365, and the **isLicensed** column displays **False** for each record. This indicates that each user was added with no license.
19. At the command prompt, type the following command and then press Enter to view the list of active users:

    ```
    Get-MsolUser
    ```

20. Verify the new users from the .csv file are included in the active users list.
21. Minimize the PowerShell window and switch back to your Edge browser.
22. In the **Microsoft 365 admin center** navigate to the **Active users** list. Review the active users and verify the new users you just imported in PowerShell appear in the list, along with Catherine Richard and Tameka Reed, who you added individually using PowerShell.
23. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all** (if necessary) to display all the menu options. Under the **Admin centers** section, select **Exchange**.
24. In the **Exchange admin center**, in the left-hand navigation pane, select **recipients**. In the **recipients** window, the **mailboxes** tab is displayed by default. Review the mailboxes. Note that no Exchange mailbox was created for any of the unlicensed users.
25. Close the **mailboxes - Microsoft Exchange** tab in your browser, which takes you back to the **Microsoft 365 admin center** tab.
26. Leave Windows PowerShell and your Edge browser open and proceed to the next task.

11.0.4 Task 4 - Configure groups and group membership by using Windows PowerShell

In a previous lab exercise, you used the Microsoft 365 admin center to create several Microsoft 365 groups. In this task, you will use PowerShell to create a group and add two members to the group.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.

2. Towards the end of the prior task, you minimized the **Windows PowerShell** window. Select the **PowerShell** icon on the taskbar to maximize the window.

3. In **Windows PowerShell**, at the command prompt type the following command and press Enter to create a new Microsoft 365 group called **Marketing department users**:

```
New-MsolGroup -DisplayName "Marketing" -Description "Marketing department users"
```

4. At the command prompt, type the following command and then press Enter to configure a variable for the group. This command will create a macro cmdlet that will retrieve all objects that belong to Marketing.

```
$MktGrp = Get-MsolGroup | Where-Object {$_.DisplayName -eq "Marketing"}
```

5. At the command prompt, type the following command and then press Enter to configure a variable for the first user account. This command will create a macro cmdlet that retrieves all users that have a display name Catherine Richard.

```
$Catherine = Get-MsolUser | Where-Object {$_.DisplayName -eq "Catherine Richard"}
```

6. At the command prompt, type the following command and then press Enter to configure a variable for the first user account. This command will create a macro cmdlet that retrieves all users that have a display name Tameka Reed.

```
$Tameka = Get-MsolUser | Where-Object {$_.DisplayName -eq "Tameka Reed"}
```

7. At the command prompt, type the following command and then press Enter to add Catherine Richard to the newly created Marketing department users group:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -GroupMemberObjectId $
```

8. At the command prompt, type the following command and then press Enter to add Tameka Reed to the newly created Marketing department users group:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -GroupMemberObjectId $
```

9. At the command prompt, type the following command and then press Enter to retrieve all members associated with the new Marketing department users group:

```
Get-MsolGroupMember -GroupObjectId $MktGrp.ObjectId
```

10. Verify that Catherine Richard and Tameka Reed appear in the list of group members for the Marketing department users group.

11. Leave Windows PowerShell open and proceed to the next task.

11.1 Task 5: Configure user passwords by using Windows PowerShell

In a previous lab, you used the Microsoft 365 admin center to update Adatum's password policy by first changing the expiration period from 90 days to 14. With a notification period of 14 days, you verified that a user who signed into Microsoft 365 received a notification message indicating their password was due to expire in 13 days. You then reset the expiration days from 14 days back to 90. For this task, you will use PowerShell to set the expiration days from 90 to 60, and the notification period from 14 days to 10.

In a previous lab, you reset a user's password using the Microsoft 365 admin center. In this task, you will change a user's password using PowerShell. You will also use PowerShell to update every user account by turning off the **Password Never Expires** parameter for all users. This will ensure that all users will be subject to the new password policy in which their password will expire after 60 days.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** account with a password of **Pa55w.rd**.

2. In **Windows PowerShell**, at the command prompt, type the following command and then press Enter to update the password policy for Adatum's **M365xZZZZZZ.onmicrosoft.com** domain. You will change the expiration period to **60 days** and the notification period to **10 days**. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

```
Set-MsolPasswordPolicy -DomainName "M365xZZZZZZ.onmicrosoft.com" -ValidityPeriod "90" -Notificati
```

3. At the command prompt, type the following command and then press Enter to change Tameka Reed's password to **P@$$W0rd**. In the command, don't forget to replace the **ZZZZZZ** with the unique tenant ID provided by your lab hosting provider.

```
Set-MsolUserPassword -UserPrincipalName "Tameka@M365xZZZZZZ.onmicrosoft.com" -NewPassword 'P@$$W0
```

4. At the command prompt, type the following command and then press Enter to turn off **Password Never Expires** parameter for all users. This will ensure that all users will be subject to the new password policy in which their password will expire after 60 days.

```
Get-MsolUser | Set-MsolUser -PasswordNeverExpires $false
```

5. Leave your Windows PowerShell session open for future lab exercises; simply minimize it before going on to the next exercise. In addition, leave your browser and all its tabs open.

Results: After completing this exercise, you should have created new users, assigned licenses, modified existing users, and configured groups and Adatum's password policies, and reset a user password by using the Windows PowerShell command-line interface.

12 Proceed to Lab 2 - Exercise 5

13 Module 2 - Lab 2 - Exercise 5 - Configuring service administrators

In this exercise, you will continue in your role as Holly Dickson, Adatum's Enterprise Administrator. As part of Adatum's Microsoft 365 pilot project, you will manage administration delegation by assigning Microsoft 365 administrator roles to several of your users. You will assign these roles using both the Microsoft 365 admin center and Windows PowerShell; this will give you experience using PowerShell to perform these administrative functions. Once you have assigned Microsoft 365 admin roles to several of the existing user accounts, you will then test those assignments by verifying the users have the permissions to act in accordance with their roles.

13.0.1 Task 1 - Assign Delegated Administrators in the Microsoft 365 Admin Center

As Holly Dickson, Adatum's Enterprise Administrator (and Microsoft 365 Global Admin), you will use the Microsoft 365 Admin Center to assign administrator rights to several users.

1. If you're not logged into the Domain Controller VM (LON-DC1) as **ADATUM\Administrator** and password **Pa55w.rd**, then please do so now.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then **Active Users**.
3. In the **Active users** list, select **Diego Siciliani**.
4. In Diego Siciliani's properties window, the **Account** tab is displayed by default. Scroll down to the **Roles** section and select **Manage roles**.
5. In the **Manage roles** window, the **User (no admin center access)** option is currently selected be default. Now that you want to assign Diego an administrator role, select the **Admin center access** option. This enables the admin roles for selection.
6. Diego has been promoted to Billing administrator, but since the Billing admin role does not appear in the list of commonly used roles, scroll down and select **Show all by category**.
7. In the list of roles that appear by category, scroll down to the **Other** category, select **Billing admin**, and then select **Save changes**.
8. On the **Manage roles** window, select the **X** in the upper-right corner of the screen to close it. This returns you to the **Active users** list.
9. Repeat steps 3-8 for **Lynne Robbins.** Assign Lynne to both the **Helpdesk admin** role and the **User admin** role (both roles are in the list of commonly used admin roles that appear under the **Admin center access** option; you do not have to select **Show all by category**).
10. Remain logged into the Microsoft 365 admin center as Holly Dickson.

13.0.2 Task 2 - Assign Delegated Administrators with Windows PowerShell

This task is similar to the prior one in that you will assign administrator rights to users; however, in this case, you will use Windows PowerShell to perform this function rather than the Office 365 Admin Center. This will give you experience performing this management function in PowerShell, since some administrators prefer

performing maintenance such as this using PowerShell. In addition, PowerShell enables you to display all the users assigned to a specific role, which can be very important when auditing your Office 365 deployment. In this task, you will learn how to use PowerShell to display all the users assigned to a specific role.

1. You should still be logged into **LON-DC1** from the prior task. Navigate to the Windows PowerShell window that you left open from the previous lab. If you closed the PowerShell window, then open an elevated instance of it using the same instruction as before.

2. You should begin by running the following command that connects your PowerShell session to the Microsoft Online Service:

   ```
   Connect-MsolService
   ```

3. In the **Sign in** dialog box that appears, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) with password **Pa55w.rd**.

4. PowerShell's execution policy settings dictate what PowerShell scripts can be run on a Windows system. Setting this policy to **Unrestricted** enables Holly to load all configuration files and run all scripts. At the command prompt, type the following command and then press Enter:

   ```
   Set-ExecutionPolicy unrestricted
   ```

   If you are prompted to verify that you want to change the execution policy, enter **A** to select **[A] Yes to All.**

5. The "official" name of all roles within Microsoft 365 includes the complete spelling of the word "administrator"; whereas, in the Office 365 admin center, "administrator" is abbreviated to "admin" simply for display purposes. When using PowerShell to perform role-related commands in the following steps, you must spell out the entire word "administrator". If you enter "admin" instead of "administrator", the command will return an error indicating that it cannot find the role.

   To view all the available roles in Microsoft 365, enter the following command in the Windows PowerShell window and then press Enter:

   ```
   Get-MsolRole |Select-Object -Property Name,Description |Out-GridView
   ```

6. Holly now wants to assign **Patti Fernandez** to the **Service support admin** role. In the Windows PowerShell window, at the command prompt, type the following command, and then press Enter:

   ```
   Add-MsolRoleMember -RoleName "Service support administrator" -RoleMemberEmailAddress PattiF@M365x
   ```

   (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)

7. You now want to verify which users have been assigned to certain roles. Displaying the users assigned to a role is a two-step process in PowerShell.

   Important: Do NOT perform the following commands just yet – this is an informational step whose purpose is to describe what you will be doing in the remaining steps in this task.

   - You will begin by running a command that creates a macro command ($role) that states that anytime $role is used in a cmdlet, it should retrieve all users assigned to whichever role name you are validating.

     ```
     $role = Get-MsolRole -RoleName "enter name of role here"
     ```

   - After creating the macro in the prior step, you will then run the following command that directs PowerShell to display all object IDs for the users who have been assigned to the name of the role that you invoked in the previous $role macro.

     ```
     Get-MsolRoleMember -RoleObjectId $role.ObjectId
     ```

8. You should now run the following two commands as described in the previous step to verify that Patti Fernandez was assigned the Service support administrator role:

   ```
   $role = Get-MsolRole -RoleName "Service support administrator"

   Get-MsolRoleMember -RoleObjectId $role.ObjectId
   ```

9. Verify that **Patti Fernandez** is in the list of users who have been assigned the **Service support administrator** role.

10. You should now run the following two commands to verify which Adatum users have been assigned to the **Billing administrator** role.

```
$role = Get-MsolRole -RoleName "Billing administrator

Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

11. Verify that **Diego Siciliani** is in the list of users who have been assigned the **Billing administrator** role (you assigned Diego to this role in the prior task using the Microsoft 365 admin center).
12. Leave your Windows PowerShell session open for future lab exercises; simply minimize it before going on to the next task.

13.0.3 Task 3 - Verify Delegated Administration

In this task, you will begin by examining the administrative properties of two users, Allan Deyoung and Lynne Robbins. You will then log into the Office 365 home page on the Client 1 VM (LON-CL1) as each user to confirm several of the changes that you made when managing their administrative delegation in the prior tasks. Finally, as Lynne Robbins, Adatum's newly assigned User Administrator, you will perform several user account maintenance tasks, such as resetting passwords and blocking a user account.

Password Note: When logging into Microsoft 365 as any of the existing user accounts that were created for you in the Microsoft 365 tenant (for example, Allan Deyoung, Lynne Robbins, and so on), you must use the same Tenant Password that you used in Lab 1 when you signed in using the tenant email account (admin@M365xZZZZZZ.onmicrosoft.com) to set up your organization profile. All the existing Microsoft 365 user accounts in your tenant have been assigned this same Tenant Password, which your instructor will provide for you.

1. In LON-DC1, you should still be logged into the Microsoft 365 admin center as Holly Dickson. If not, then do so now.
2. In the **Microsoft 365 admin center**, if you are not displaying the **Active users**, then navigate to there now.
3. In the **Active users** list, select **Allan Deyoung**.
4. In **Allan Deyoung's** properties window, the **Account** tab is displayed by default. Under the **Roles** section, it should indicate that Allan has **No administrator access**. Select the **X** in the upper right corner to close Allan's properties window.
5. In the **Active users** list, select **Lynne Robbins**.
6. In **Lynne Robbins's** properties window, it should indicate that Lynne has been assigned the **User admin** and **Helpdesk admin** roles. Close Lynne's properties window.
7. Switch to **LON-CL1**.
8. On the log-in screen, you will log in as the **Administrator** account with a password of **Pa55w.rd**.
9. If a **Networks** window appears, select **Yes**.
10. On the taskbar, select the **Microsoft Edge** icon.
11. In your **Edge** browser navigate to **https://portal.office.com**.
12. You will begin by signing into Office 365 as **Allan Deyoung**. In the **Sign-in** window, enter **AllanD@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). In the **Enter password** window, enter the Tenant Password provided by your lab hosting provider.
13. On the **Stay signed in?** window, select **Yes**.
14. If a **Get your work done with Office 365** window appears, select the **X** to close it.
15. In the **Microsoft Office Home** page, if an **Office 365 apps** box appears below the **Install Office** button, select **Got it!** to close the box. Note how the **Admin** option is not available.

    You have just verified that Allan cannot access the Microsoft 365 admin center since he was never assigned an administrator role.
16. In **Microsoft Edge**, at the top right of the **Microsoft Office Home**, select the user icon for **Allan Deyoung** (the circle in the upper right-hand corner with Allan's picture in it), and in his **My account** pane, select **Sign out.**

17. You will now sign into Office 365 as **Lynne Robbins**. In your current **Edge** browser tab, it should display a message indicating **Allan, you're signed out now**. In this window, it gives you the option of signing back in as Allan, or signing in as a different user. Select **Switch to a different account**, and in the **Email address** field that appears, enter **LynneR@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and then select **Sign in**. In the **Enter password** window, enter the Tenant Password provided by your lab hosting provider.

18. Select **Yes** on the **Stay signed in?** window.

19. In the **Microsoft Office Home** page, if an **Office 365 apps** box appears below the **Install Office** button, select **Got it!** to close the box. Since Lynne has been assigned to an administrator role, note how **Admin** appears in the **Microsoft Office Home** page. Select the **Admin** option.

20. On the **Microsoft 365 admin center**, select **Users** on the left-hand navigation pane and then select **Active users**.

21. As the **Helpdesk administrator**, Lynne has permission to change user passwords. Lynne was recently contacted by **Diego Siciliani** and **Allan Deyoung**, each of whom reported that their passwords may have been compromised. Per Adatum's company policy, Lynne must reset their passwords to a temporary value, and then force them to reset their password at their next login.

    In the **Active users** list, as you move your mouse from one user account to another, notice the **key (Reset a password)** icon that appears to the right of each user's name. Select the key icon that appears to the right of **Diego Siciliani's** name.

22. In the **Reset password** window for Diego, select the **Let me create the password** option, and then enter **P@$$w0rd** in the **Password** field. If necessary, select the **Require this user to change their password when they first sign in** check box so that it displays a check mark.

23. Select **Reset**.

24. You should receive an error message indicating that you cannot reset Diego's password because he has been assigned an admin role. In Diego's case, he was assigned to the Billing Admin role. Since only Global Admins can change another admin's password, Lynne will need to ask Holly Dickson to make this change. Select **Close**.

25. If a survey request window appears, select **Cancel**.

26. In the **Active users** list, select the **key (Reset a password)** icon for **Allan Deyoung**.

27. In the **Reset password** window for Allan, select the **Let me create the password** option, and then enter **P@$$w0rd** in the **Password** field. If necessary, select the **Require this user to change their password when they first sign in** check box so that it displays a check mark.

28. Select **Reset**.

29. On the **Reset password** window, you should receive a message indicating the password was successfully reset. Select the **Send password in email** check box. This displays an **Email the new password to the following recipients** field, which displays Lynne Robbins' email address. Since you also want to email this temporary password to Allan, you should enter Allan's email address following Lynne's.

    If you enter multiple email addresses, they must be separated by a semicolon and a space, so enter a semicolon and a space following Lynne's email address, enter Allan's email address of **AllanD@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider), and then select **Send email and close**.

30. Management has recently discovered that Alex Wilber's username may have been compromised. As a result, Lynne has been asked to block Alex's account so that no one can sign in with his username until management is able to determine the extent of the issue. In the **Active users** list, select the circle to the left of **Alex Wilber's** name (do NOT select Alex's name itself).

    Note: If any other user account is selected, you must unselect that user account before proceeding. Check Allan Deyoung's account, since you just reset his password; uncheck his account if necessary. Only Alex's account should be selected.

31. In the menu bar at the top of the page, select the **ellipsis icon (...)** to display a drop-down menu of additional options. In the menu that appears, select **Edit sign-in status**.

32. In the **Block sign-in** window, select the **Block this user from signing in** check box, and then select **Save**.

33. The **Block sign-in** window should display a message indicating that Alex is now blocked from signing in (and no one can sign in with Alex's username in the event that his username was actually compromised). In addition, Alex will automatically be signed out of Microsoft services within 60 minutes. Select the **X** in the upper right-hand corner of the window to close it.

34. Lynne has just been informed that Nestor Wilke's username has also been potentially compromised. Repeat steps 30 through 33 to block Nestor from signing in (and to block anyone else from using his username to sign in).

35. When you tried to block Nestor's sign in, you should have received an error message indicating **Changes could not be saved**. The reason that you received this error is that Nestor is a Global Admin, and Lynne is not. Only a Global Admin can block another Global Admin from being able to sign in. Lynne will need to ask Holly Dickson to make this change.

36. To verify whether Alex Wilber can sign in after you blocked his account, you will attempt to sign in as Alex. Log out of Microsoft 365 by selecting the user icon for **Lynne Robbins** (the circle with Lynne's picture in the upper right-hand corner), and in her **My account** pane, select **Sign out.**

37. As a best practice, close all your browser tabs except for the **Sign out** tab once you have been signed out. On the **Sign out** tab, navigate to **https://portal.office.com**.

38. In the **Pick an account** window, select **Use another account**. In the **Sign in** window, enter **AlexW@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). In the **Enter password** window, enter the Tenant Password provided by your lab hosting provider.

    The **Pick an account** window should appear, and it should display an error message indicating **Your account has been locked. Contact your support person to unlock it, then try again.**

    You have just verified that Alex (or someone who has obtained Alex's username and password) cannot log in.

39. Switch back to LON-DC1, where you should still be logged into **Microsoft 365** as Holly Dickson. The **Active users** list should be displayed in the **Microsoft 365 admin center** from earlier in this task.

40. Upon further investigation, Adatum's CTO has determined that Alex Wilber's account has, in fact, not been compromised; therefore, the CTO has asked Holly to remove the block on Alex's sign in. Repeat steps 30 through 33 to unblock his account. Note how the **Block sign-in** window from step 32 now displays the **Unblock sign-in** window instead.

    In the **Unblock sign-in** window, the **Block this user from signing in** check box is currently selected. Select this check box to clear it, select **Save changes**, and once Alex has been unblocked from signing in, close this window.

41. Leave your browser and all tabs open and proceed to the next lab.

14 End of Lab 2

15 Module 3 - Lab 3 - Exercise 1 - Running the Microsoft 365 connectivity analyzer tools

The Remote Connectivity Analyzer is a web-based tool that's designed to help IT administrators troubleshoot connectivity issues with their Office 365 and Exchange Online deployments. In your role as Holly Dickson, Adatum's Enterprise Admin, you want to run the tool to determine if you have any connectivity issues that may disrupt your Microsoft 365 deployment.

15.0.1 Task 1: Run the Microsoft Connectivity Analyzer tool

In this task, you will use the Remote Connectivity Analyzer tool to perform the following connectivity tests:

- You will test the external domain name settings for your verified **M365xZZZZZZ.onmicrosoft.com** domain in Office 365. The test will look for issues with mail delivery such as not receiving incoming email from the Internet and Outlook client connectivity issues that involve connecting to Outlook and Exchange Online.
- You will perform a test that walks through the steps Outlook uses to connect from the Internet. This test verifies connectivity using both the RPC over HTTP protocol and the MAPI over HTTP protocol.

This tools also includes a link to download the Microsoft Support and Recovery Assistant, which you will test in the next task.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior lab exercise.
2. At the end of your prior lab exercise, you logged out of Microsoft 365 as Ada Russell and you closed your Microsoft Edge browser. In this task, re-open a new instance of your Edge browser by selecting the **Edge** icon on your taskbar.
3. In your Edge browser, enter the following URL in the address bar: **https://testconnectivity.microsoft.com**
4. Test #1 - You will begin by testing Office 365 connectivity.

   On the **Microsoft Remote Connectivity Analyzer** page, in the left-hand navigation pane, the **Office 365** tab is displayed by default.
5. On the **Office 365** page, select the box that says: **Help Identify My Issue with Exchange DNS**.
6. On the **Office 365 Exchange Domain Name Server (DNS) Connectivity Test** page, enter the following information:
   - Enter **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) in the **Domain Name** field
   - Under **Service Selection**, select the **Office 365 (Default)** option (if it's not already selected)
   - Under **Verification**, enter the characters that you can see in the verification field and then select **Verify**. Note - The verification code is not case-sensitive.
7. If the verification test is successful, a message will be displayed below the verification field that indicates: **You are now verified for the rest of this browser session (30 minute maximum).**
8. Select **Perform Test**.

   Note: If you receive a message about having performed too many tests in 60 seconds, wait a couple of minutes and then repeat the test.
9. When you see **Successfully verified specified external domain name settings for your domain in Office 365**, select the arrow next to **Test Steps** (selecting on **Test Steps** itself does not work) and then review the connectivity checks that were made against the **M365xZZZZZZ.onmicrosoft.com** domain.
10. Test #2 - You will next test Exchange Server connectivity.

    On the **Microsoft Remote Connectivity Analyzer** page, in the left-hand navigation pane, select **Exchange Server**.
11. On the **Exchange Server** page, select the box that says: **Outlook Connectivity**.
12. On the **Outlook Connectivity** page, enter the following information:
    - Enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) in BOTH the **Email Address** and **Domain\User Name (or UPN)** fields
    - Copy and paste in the password of the Microsoft 365 tenant admin in the **Password** field
    - Select the **Use Autodiscover to detect server settings** option
    - Select the check box that says: **I understand that I must use the credentials of a working account from my Exchange domain to be able to test connectivity to it remotely. I also acknowledge that I am responsible for the management and security of this account**.
13. Select **Perform Test**.
14. When you see **The Outlook connectivity test completed successfully** message, select the arrow next to **Test Steps** (selecting on **Test Steps** itself does not work) and then review the connectivity checks that were made against **Outlook**. Each step has additional **Test Steps** that you can select to displayed more detailed information about each test.
15. Leave the **Microsoft Remote Connectivity Analyzer** window open in your Edge browser and proceed to the next task.

15.0.2 Task 2 - Run the Microsoft 365 Support and Recovery Assistant

The Microsoft Support and Recovery Assistant (SARA) works by running tests to figure out what's wrong and offers the best solution for the identified problem. It can currently fix Office, Microsoft 365, and Outlook

problems. If the Microsoft Support and Recovery Assistant can't fix a problem, it will suggest next steps and help you get in touch with Microsoft support.

In this task, you will download the SARA tool and then you will run it to check for authentication checks for Exchange Online.

1. You should still be logged into the **LON-CL1** VM as the **Administrator** from the prior task.
2. You should still have the **Microsoft Remote Connectivity Analyzer** window open in your Edge browser. In the left-hand navigation pane, select **SARA Client**. This will open a new tab in your browser that displays the **About the Microsoft Support and Recovery Assistant** page.
3. In the **About the Microsoft Support and Recovery Assistant** page, select the **Download** button in step #1. This will automatically download the **SaraSetup.exe** file.
4. If the **SaraSetup.exe** file appears in the notification bar at the bottom of the screen, select **Open file** after the download is complete to initiate the installation wizard.

   Note: If the notification bar does not appear at the bottom of the screen, then select the **File Explorer** icon on the taskbar to open **File Explorer**, select the **Downloads** folder, and then double-click on the **SaraSetup.exe** file to initiate the installation wizard.
5. In the **Microsoft Support and Recovery Assistant Setup** wizard, on the **Do you want to install this application?** page, select **Install**.
6. In the **Microsoft Support and Recovery Assistant Setup** window, once the wizard finishes downloading the application, it will display the license agreement page. Select **I agree**.
7. On the **Which app are you having problems with?** page, select **Advanced diagnostics** and then select **Next**.
8. On the **Which Advanced diagnostic would you like to run?** page, select **Exchange Online** and then select **Next**.
9. On the **Select the diagnostic you'd like to run** page, select **Perform authentication checks** and then select **Next**.
10. On the next page that asks if this is the affected machine, select **Yes** and then select **Next**.
11. On the **Let's get started fixing your problem** page, enter **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and enter **Pa55w.rd** in the **Password** field. Select the **Keep me signed in** check box (is it's not already checked) and then select **Next**.
12. Once the **Microsoft 365 Support and Recovery Assistant** generates the diagnostic test results, review the details by selecting **+ View summary**. Select the down arrow to the far-right of **Office 365 readiness checks** to review the specific tests that were performed. Also note the domain registration check that was performed using Holly's account.
13. Close the **Microsoft 365 Support and Recovery assistant** window (if you select the **Next** button, it will take you to a survey page).

    Note: If selecting the X in the upper-right hand corner of the SARA window does not close it, right click on the SARA icon on the taskbar and select the **Close window** option.
14. Close your Edge browser and proceed to the next lab exercise.

16 Proceed to Lab 3 - Exercise 2

17 Module 3 - Lab 3 - Exercise 2 - Connecting Office 2016 clients

Microsoft 365 is designed to enable customers all over the world to connect to the service using an internet connection. As the service evolves, the security, performance, and reliability of Microsoft 365 are improved based on customers using the internet to establish a connection to the service. Customers planning to use Microsoft 365 should assess their existing and forecasted internet connectivity needs as a part of the deployment project. For enterprise class deployments, reliable and appropriately sized internet connectivity is a critical part of consuming Microsoft 365 features and scenarios.

Network evaluations can be performed by many different people and organizations depending on your size and preferences. The network scope of the assessment can also vary depending on where you're at in your deployment process. Holly Dickson, Adatum's Enterprise Administrator, wants to being assessing Microsoft 365 network connectivity for Adatum. In this task, she will begin her assessment by verifying that different users can log into Outlook 2016 and connect to Exchange Online from different client PC's.

17.1 Task 1: Verify that Outlook 2016 can connect to Microsoft 365

In this task, you will begin in LON-CL1, where you will log into Outlook 2016 as the MOD Administrator and you will verify that you are connected to Exchange Online. You will then switch to LON-CL2, where you will repeat these steps, this time logged in as Holly Dickson.

1. On **LON-CL1**, select the Windows icon in the lower left corner of the taskbar to display the Start menu. Scroll down through and menu and select **Outlook 2016**. This initiates the Outlook 2016 setup wizard.
2. On the **Welcome to Outlook 2016** window, select **Next**.
3. On the **Add an Email Account** page, the **Do you want to set up Outlook to connect to an email account?** option is set to **Yes** by default. Accept this default setting by selecting **Next**.
4. On the **Auto Account Setup** page, enter the following information, and then Select **Next**:
   - Your Name: **MOD Administrator**
   - E-mail Address: **admin@M365xZZZZZZ.onmicrosoft.com** (replace ZZZZZZ with the tenant ID provided by your lab hosting provider)
   - Password: copy and paste in the tenant password provided by your lab hosting provider
   - Retype Password: copy and paste in the tenant password provided by your lab hosting provider
   - Manual setup or additional server types - do not select this option
5. Select **Next**. The wizard will begin configuring Outlook 2016.
6. During the configuration process, Outlook will attempt to make an encrypted connection to the Exchange Online mail server using the MOD Administrator's email address. An **Enter password** dialog box will appear that asks you to enter the password for the **admin@M365xZZZZZZ.onmicrosoft.com** account. Copy and paste in the tenant password provided by your lab hosting provider and then select **Sign in**.
7. Once the configuration is complete and a message is displayed indicating your email account was successfully configures and is ready to use, select **Finish**.
8. The **Microsoft Office Activation Wizard** will begin. Select **Close**.
9. In the **First things first** dialog box, Select **Ask me later** and then select **Accept**.
10. Verify that you are connected to Exchange Online by creating a new email message and sending it to Holly Dickson's email account. On the ribbon at the top of the page, select **New Email**. In the new email message form, select **To**, and then in the **Global Address List** select **Holly Dickson**, select **To**, and then select **OK**. Enter **Test message** in the **Subject** line and the body of the message and then select **Send**.
11. Switch to **LON-CL2**. Log in as the **Admin** with a password of **Pa55w.rd**.
12. If a **Networks** pane appears, select **Yes** to allow the PC to be discoverable by other PCs on this network.
13. 2. Open **Microsoft Edge** . In your browser go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**
14. In the **Pick an account** window, select **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your tenant ID provided by your lab hosting provider).
15. In the **Enter password** dialog box, enter **Pa55w.rd** and then select **Sign in**.
16. In the **Microsoft Office Home** page, select **outlook**, which opens the office 365 Outlook.
17. Once Outlook is open, verify in Holly's **Inbox** that she received the email from the **MOD Administrator** that you just sent to her. In turn, reply to the email by sending a Reply message back to the **MOD administrator**.
18. Close Outlook on LON-CL2.

19. Switch back to LON-CL1.
20. Verify that Holly's reply is received into the MOD Administrator's Inbox in Outlook. By configuring Outlook for the MOD Admin's mailbox and Holly's mailbox and sending emails back and forth between the two users using two different PCs, you have verified that Outlook is connected to Exchange Online in Microsoft 365 and that an encrypted connection to your mail server is available.
21. Close Outlook on LON-CL1.

18 Module 4 - Lab 4 - Exercise 1 - Preparing for directory synchronization

As in the previous lab exercises you will take on the role of Holly Dickson, Adatum Corporation's Enterprise Administrator. Adatum has recently subscribed to Microsoft 365, and you have been tasked with deploying the application in Adatum's virtualized lab environment. In this lab, you will perform the tasks necessary to manage your Microsoft 365 identity environment using both the Microsoft 365 admin center and Windows PowerShell.

During this exercise you will set up and manage Azure AD Connect. You will create on-premises users and validate the sync process so that their identities are moved to the cloud. Some of the steps may feel familiar from previous exercises; however, in this case they are needed to validate the synchronization process.

18.0.1 Task 1: Configure your UPN suffix

In Active Directory, the default User Principal Name (UPN) suffix is the DNS name of the domain where the user account was created. The Azure AD Connect wizard uses the UserPrincipalName attribute, or it lets you specify the on-premises attribute (in a custom installation) to be used as the user principal name in Azure AD. This is the value that is used for signing into Azure AD.

If you recall, your VM environment was created by your lab hosting provider with an on-premises domain titled **adatum.com**. This domain included a number of on-premises user accounts, such as Holly Dickson, Laura Atkins, and so on. Then in the first lab in this course, you finished provisioning a custom domain which your lab hosting provider created for Adatum titled **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx was the unique UPN name assigned to your tenant, and xxxCustomDomainxxx.xxx was the name your lab hosting provider assigned to the custom domain).

In this task, you will use PowerShell to change the user principal name of the domain for the entire Adatum Corporation by replacing the originally established **adatum.com** domain with the custom **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain. In doing so, you will update the UPN suffix for the primary domain and the UPN on every on-premises user account in AD DS with **@xxxUPNxxx.xxxCustomDomainxxx.xxx**.

A company may change its domain name (also known as a vanity domain name) for a variety of reasons. For example, a company may purchase a new domain name, or a company may change its name and it wants its domain name to reflect the new company name, or a company may be sold and it wants its domain name to reflect the new parent company's name. Regardless of the underlying reason, the goal of changing a domain name is typically to change the domain name on each user's email address.

For this lab, Adatum has purchased a new domain (provided by your lab hosting provider); therefore, it wants to change the domain name of all its users' email addresses from @adatum.com to @xxxUPNxxx.xxxCustomDomainxxx.xxx.

1. Switch to **LON-DC1** where you should still be logged in as **ADATUM\Administrator** and password **Pa55w.rd**.
2. You must now open **Windows PowerShell**. Select the magnifying glass (**Search**) icon on the taskbar at the bottom of the screen and type **powershell** in the Search box that appears. In the menu that appears, right-click on **Windows PowerShell** and select **Run as administrator** in the drop-down menu.
3. Using **Windows PowerShell**, you must replace the on-premises **adatum.com** domain with the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain (where you will replace xxxUPNxxx with the unique UPN name assigned to your tenant, and you will replace xxxCustomDomainxxx.xxx with the custom domain created by your lab hosting provider). In doing so, you will update the UPN suffix for the primary domain and the UPN on every user in AD DS with **@xxxUPNxxx.xxxCustomDomainxxx.xxx**.

In the following Powershell command, the **Set-ADForest** cmdlet modifies the properties of an Active Directory forest, and the **-identity** parameter specifies the Active Directory forest to modify. To perform this task, run the following command to set the **UPNSuffixes** property for the **adatum.com** forest (remember to change xxxUPNxxx to your unique UPN name and xxxCustomDomainxxx.xxx to your lab hosting provider's custom domain name):

```
Set-ADForest -identity adatum.com -UPNSuffixes @{replace="xxxUPNxxx.xxxCustomDomainxxx.xxx"}
```

4. You must then run the following command that changes all existing adatum.com accounts to the new xxxUPNxxx.xxxCustomDomainxxx.xxx domain (remember to change xxxUPNxxx to your unique UPN name and xxxCustomDomainxxx.xxx to your lab hosting provider's custom domain name):

   Get-ADUser -Filter * -Properties SamAccountName | ForEach-Object { Set-ADUser $_ -UserPrincipalName ($_.SamAccountName + "@xxxUPNxxx.xxxCustomDomainxxx.xxx")}

5. You will continue using PowerShell on LON-DC1 in the next task.

18.0.2 Task 2: Prepare problem user accounts

Integrating your on-premises Active Directory with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. However, errors can occur when identity data is synchronized from Windows Server Active Directory (AD DS) to Azure Active Directory (Azure AD).

For example, two or more objects may have the same value for the **ProxyAddresses** attribute or the **UserPrincipalName** attribute in on-premises Active Directory. There are a multitude of different conditions that may result in synchronization errors. Organizations can correct these errors by running Microsoft's IdFix tool, which performs discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory.

In this task, you will run a script that breaks various Adatum on-premises user accounts. As part of your Adatum pilot project, you are purposely breaking these identity objects so that you can run the IdFix tool in the next task to see how it fixes the broken accounts.

1. On LON-DC1, in the Windows PowerShell window, run the following command to change the root source to **C:\labfiles** so that you can access any files from that location:

   ```
   CD C:\labfiles\
   ```

2. PowerShell's execution policy settings dictate which PowerShell scripts can be run on a Windows system. Setting this policy to **Unrestricted** enables Holly to load all configuration files and run all scripts. At the command prompt, type the following command, and then press Enter:

   ```
   Set-ExecutionPolicy Unrestricted
   ```

3. You will then be prompted to confirm the execution policy change. Type **A** and press Enter to select the **[A] Yes to All** option.

4. Enter the following command that runs a PowerShell script that creates problem user accounts. This script is stored in the **C:\labfiles** folder. The users that are included in this script purposely have issues with their user accounts; this will enable you to troubleshoot these accounts in the next task using the IdFix tool.

   ```
   .\CreateProblemUsers.ps1
   ```

   Note: Wait until the script has completed before proceeding to the next task. This Windows PowerShell script will make the following changes in AD DS:

   - **Klemen Sic**. Update the UserPrincipalName for Klemen to include an extra "@" character.
   - **Lara Raisic**. Update the emailAddress attribute for Lara to **lara@adatum.com**.
   - **Logan Boyle**. Update the emailAddress attribute for Logan to **logan@adatum.com**.
   - **Maj Hojski**. Update the emailAddress attribute for Maj to blank characters (" ").

5. Close PowerShell.

18.0.3 Task 3: Run the IdFix tool and fix identified issues

In this task you will download and use the IdFix tool to fix the user accounts that were broken in the previous task. Running the IdFix tool will correct any user account errors prior to synchronizing identity data between your on-premises environment and Azure AD.

1. You should still be logged into **LON-DC1** as the **Administrator** from the prior task.
2. In your **Microsoft Edge** browser, you should still be logged into Microsoft 365 as the **MOD Administrator** (**admin@M365xZZZZZZ.onmicrosoft.com**). You should have tabs open for the **Microsoft Office Home** page and the **Microsoft 365 admin center**.

   In your **Edge** browser, open a new tab and then enter the following URL in the address bar to access the Office 365 page for the IdFix Directory Synchronization Error Remediation Tool:

   https://microsoft.github.io/idfix/installation/
3. On the **Microsoft - IdFix** window, under the **Installation** section at the top of the page, the instructions direct you to run **setup.exe** to install the IdFix application on your machine. Select **setup.exe** to download the file to LON-DC1.
4. Once the **setup.exe** file is downloaded, it will appear in the notification bar at the bottom of the screen. Select **Open file**.
5. In the **Do you want to run this file?** dialog box, select **Run**.
6. In the **Do you want to install this application?** dialog box, select **Install**.
7. In the **Do you want to run this file?** dialog box, select **Run**.
8. In the **IdFix Privacy Statement** message box, select **OK**.
9. In the **IdFix** window that appears, on the menu bar at the very top of the screen, select **Query** to query the directory. After a short wait, you should see several errors.
10. Select the **ERROR** column heading to sort the records by error in alphabetical error.

    Note: If any **topleveldomain** errors appear, then ignore them as they cannot be fixed by the IdFix tool.
11. If you will recall, in the script that broke the users' accounts, Maj Hojski's email address attribute was set to all blank characters. In the row indicating blank characters, this is **Maj Hojski** row. Select the drop-down arrow in the **ACTION** field and select **EDIT**.
12. In the **Klemen Sic** row, select the drop-down arrow in the **ACTION** field and select **EDIT**.
13. On the menu bar at the top of the window, select **Apply**.
14. In the **Apply Pending** dialog box that appears, select **Yes**.

    Note: Notice that the value in the **Action** column changed from **EDIT** to **COMPLETE** for these two users; this indicates that IdFix updated the two user objects and corrected the errors.
15. Select the **File Explorer** icon on the taskbar.
16. In the **C:\Deployment Tools\IdFix** folder, double-click the **Verbose {date} {time}.txt** file to open **Notepad** and view the updated transactions in the transaction log. Maximize the **Notepad** window and locate the three **Update** transactions that appear at the bottom of the file; these transactions reflect the updates you just initiated. When you have finished reviewing this log file, close Notepad.
17. Select the **IdFix tool** icon on the taskbar.
18. On the menu bar at the top of the window, select **Query** to refresh the query results.
19. In the query results, note how one of the two users who you just fixed no longer appears in the results (Klemen). The exception is **Maj Hoski**. When you originally broke Maj's account by running the script in the prior task, it replaced her email address with blank characters. Then when you flagged her account to be edited in the earlier step, the IdFix tool replaced the blank characters with Maj's name. Now you need to fix this value by replacing her name with her actual email address.

    Find the **Maj Hoski** row. Note how the **VALUE** for Maj is her name rather than her email address. To fix this email attribute for Maj, you must first select the **MajHojski** value in the **UPDATE** column and then replace it by typing **maj@adatum.com**. Then select the drop-down arrow in the **ACTION** field and select **EDIT**.

20. Find the **Logan Boyle** row. Note how the **VALUE** for Logan was incorrectly entered as **Lara@adatum.com**, which resulted in a duplicate error because this is the same email address as Lara Raisic, which appears above it.

    To fix this email attribute for Logan, you must first select the **[E]Lara@adatum.com** value in the **UPDATE** column for Logan and then replace it by typing **logan@adatum.com**. Then select the drop-down arrow in the **ACTION** field and select **EDIT**.

21. On the menu bar at the top of the window, select **Apply**.

22. In the **Apply Pending** dialog box that appears, select **Yes**.

    Note: This will update the two user objects and correct their UPN.

23. On the menu bar, select **Query**. In the query results, note how the two users who you just fixed no longer appear in the results.

    Note: If a dialog box appears indicating an unhandled exception has occurred, select **Continue**.

    As you can see, there are two users whose errors you have not fixed (**An Dung Dao** and **Ngoc Bich Tran**). We are purposely leaving these errors alone so that you can see what happens during the synchronization process using the Azure AD Connect tool in the next exercise when it processes users with these conditions.

    Important: When there are format and duplicate errors for distinguished names, the **UPDATE** column either contains the same string as the **VALUE** column (which is the case for these two final users), or the **UPDATE** column entry is blank. In either case, this means that IdFix cannot suggest a remediation for the error. You can either fix these errors outside IdFix, or manually remediate them within IdFix. You can also export the results and use Windows PowerShell to remediate many errors.

24. Close the IdFix and File Explorer windows.

18.0.4 Task 4: Prepare for Directory Synchronization

The Azure Active Directory Connect synchronization service is a main component of Azure AD Connect. It's responsible for processing all operations related to synchronizing identity data between your on-premises environment and Azure AD. The sync service consists of an on-premises component (Azure AD Connect sync) and a cloud service component (Azure AD Connect sync service).

Before you can run Azure AD Connect, you must first configure several settings that control the synchronization process, which you will do in this task. Once you have completed the preparation process, you will then run the Azure AD Connect tool in the next exercise.

1. You should still be logged into **LON-DC1** as the **Administrator** from the prior task.

2. You want to begin by adding several trusted sites for Microsoft Edge. If you're familiar doing this with Internet Explorer, the process is basically the same for Edge; however, the location of the **Security** settings is different. With IE, you added trusted sites through IE's Internet Options; for Edge, you will add trusted sites through the Windows Control Panel.

    Select the magnifying glass icon on the taskbar and then enter **control** in the Search box.

3. In the list of search results, select **Control Panel**.

4. In the **Control Panel**, select **Network and Internet**.

5. On the **Network and Internet** window, select **Internet Options**.

6. This opens the **Internet Properties** window. Select the **Security** tab.

7. The **Internet** zone should be selected by default. Towards the bottom of the window, select the **Custom Level** button.

8. In the **Security Settings – Internet Zone** window, scroll down to the **Downloads** section. The first option in this section is **File download**. Verify the **File download** option is set to **Enable** and then select **OK**.

9. This takes you back to the **Internet Options** window. Select the **Trusted sites** zone.

10. In the **Trusted Sites** zone, you must add several sites. Select the **Sites** button.

11. In the **Trusted sites** window, in the **Add this website to the zone** field, enter the following URL and then select **Add**: **https://outlook.office365.com/**

12. Repeat step 11 to add the following site: **https://outlook.office.com/**
13. Repeat step 11 to add the following site: **https://portal.office.com/**
14. Select **Close** once you have added these three sites.
15. In the **Internet Options** window, select **OK** to close the window.
16. Close the **Network and Internet** window.
17. Proceed to the next exercise. You are now ready to install the Azure AD Connect tool and enable synchronization.

19 Proceed to Lab 4 - Exercise 2

20 Module 4 - Lab 4 - Exercise 2 - Perform Directory Synchronization

In this exercise, you will enable synchronization between Adatum's on-premises Active Directory and Azure Active Directory. Azure AD Connect will then continue to synchronize any delta changes every 30 minutes. You will then make some group updates and then manually force an immediate synchronization rather than waiting for Azure AD Connect to automatically synchronize the updates. You will then verify whether the updates were synchronized.

Important: When you start this exercise, you should perform the first three tasks without any delay between them so that Azure AD Connect does not automatically synchronize the changes that you make to the identity objects.

20.0.1 Task 1 - Install Azure AD Connect and Initiate Synchronization

In this task, you will run the Azure AD Connect setup wizard to enable synchronization between Adatum's on-premises Active Directory and Azure Active Directory. Once the configuration is complete, the synchronization process will automatically start.

1. You should still be logged into **LON-DC1** as the **Administrator** from the prior task.
2. After finishing the previous lab exercise, you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.
3. In your **Edge** browser, select the **Microsoft 365 admin center** tab, and then in the left-hand navigation pane, select **Users**, and then select **Active Users**.
4. In the **Active users** window, on the menu bar, select the **ellipsis** icon (to the right of **User templates**), and then in the drop-down menu, select **Directory synchronization**.
5. In the **Active Directory preparation** window, select **Download Microsoft Azure Active Directory Connect tool**. This opens a new tab in your browser and takes you to the Microsoft Download Center.
6. In the **Microsoft Download Center**, scroll down to the **Microsoft Azure Active Directory Connect** section and select **Download**.
7. In the notification bar at the bottom of the screen, once the **AzureADConnect.msi** file has finished downloading, select **Open file**.
8. In the **Do you want to run this file?** dialog box, select **Run**.
9. This initiates the installation of the Microsoft Azure Active Directory Connect Tool. If the **Welcome to Azure AD Connect** window does not appear on the desktop, find the icon for it on the taskbar (it will be the final icon on the right) and select it.

   On the **Welcome to Azure AD Connect** window in the setup wizard, select the **I agree to the license terms and privacy notice** check box and then select **Continue**.
10. On the **Express Settings** page, read the instruction regarding a single Windows Server AD forest and then select **Use express settings**.
11. On the **Connect to Azure AD** window, enter **Holly@M365xZZZZZZ.onmicrosoft.com** (where zzzzzz is the tenant ID provided by your lab hosting provider) in the **USERNAME** field, enter **Pa55w.rd**

in the **PASSWORD** field, and then select **Next** (you may have to select **Next** twice; once to enable it and again to proceed).

12. On the **Connect to AD DS** page, enter **adatum\Administrator** in the **USERNAME** field, enter **Pa55w.rd** in the **PASSWORD** field, and then select **Next** (you may have to select **Next** twice; once to enable it and again to proceed).
13. In the **Azure AD sign-in configuration** window, select the **Continue without matching all UPN suffixes to verified domains** check box at the bottom of the page, and then select **Next**.
14. On the **Ready to configure** screen, select the check box for **Start the synchronization process when configuration completes** if it's not already selected, and then select **Install**.
15. Wait for the configuration to complete and then select **Exit**.
16. Select the **Windows (Start)** icon in the lower left corner of the taskbar. In the **Start** menu that appears, select **Azure AD Connect** to expand the group, and then select **Synchronization Service** to start this desktop application.

    Note: If you selected **Azure AD Connect** in the **Start** menu and it expanded and you were able to select **Synchronization Service**, then proceed to the next step. However, if **Azure AD Connect** did not expand when you selected it in the **Start** menu, then you will need to close all applications and then restart LON-DC1. The remaining instruction in this step is what to do if you needed to restart LON-DC1.

    After LON-DC1 restarts, follow the instructions from your lab hosting provider to select **Ctrl+Alt+Delete**. This will display the log on screen for LON-DC1.

    Log in as **Adatum\Administrator** with a password of **Pa55w.rd**. Minimize **Server Manager** after it opens, and then open **Edge** and navigate to **https://portal.office.com**. Log in as **Holly@M365xZZZZZZ.onmicrosoft.com** with a Password of **Pa55w.rd**. On the **Microsoft Office Home** page, select **Admin** to open the **Microsoft 365 admin center**.

    Then select the **Windows (Start)** icon in the lower left corner of the taskbar. In the **Start** menu that appears, select **Azure AD Connect** to expand the group (this time it should expand), and then select **Synchronization Service**.
17. In the **Synchronization Service Manager** window, the **Operations** tab at the top of the screen is displayed by default so that you can monitor the synchronization process.
18. Wait for the **Export** profile to complete for **M365xZZZZZZ.onmicrosoft.com**; when it finishes, its **Status** should be **completed-export-errors**. Once it's complete and you see this status, select this row.
19. In the bottom portion of the screen, a detail pane appears showing the detailed information for this operation.

    - In the **Export Statistics** section, note the number of users that were added and the number that were updated.
    - In the **Export Errors** section, note the errors that appear. If you recall back in the prior lab exercise when you ran the IdFix tool, there were two users with validation errors that you purposely did not fix (**Ngoc Bich Tran** and **An Dung Dao**). Select the links under the **Export Errors** column and you will see that these are the two users that were not synchronized by the Azure AD Connect tool due to these data validation errors.

    Note: Because a synchronization had not been performed prior to this, the initial synchronization was a **Full Synchronization** (see the **Profile Name** column). Because the synchronization process will continue to run automatically every 30 minutes, any subsequent synchronizations will display **Delta Synchronization** as its **Profile Name**. If you leave the **Synchronization Service Manager** window open, after 30 minutes you will see that it attempts to synchronize the two users who were not synchronized during the initial synchronization. These will display as a **Delta Synchronization**.
20. Now that you have seen Azure AD Connect complete a Full Synchronization, in the next task you will make some updates and manually force an immediate synchronization rather than waiting for it to synchronize updates every 30 minutes. Close the **Synchronization Service Manager**.
21. In your browser, close all tabs except for the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab.
22. Leave LON-DC1 open as it will be used in the next exercise.

20.0.2 Task 2 - Create Group Accounts to Test Synchronization

To test the manual, forced synchronization process, you will also set up several group scenarios to verify whether the forced synchronization function is working in Azure AD Connect. You will create a new security group, and you will update the group members in an existing, built-in security group, all within Adatum's on-premises environment.

Each group will be assigned several members. After the forced synchronization, you will validate that you can see the new security group in Microsoft 365 and that its members were synced up from the on-premises group to the cloud group. You will also validate that you can NOT see the built-in security group in Microsoft 365, even though you added members to it in Adatum's on-premises environment. Built-in groups are predefined security groups that are located under the Builtin container in Active Directory Users and Computers. They are created automatically when you create an Active Directory domain, and you can use these groups to control access to shared resources and delegate specific domain-wide administrative roles. However, they are not synchronized to Microsoft 365, even after adding members to them within their on-premises AD group. You will validate this functionality in this task.

1. You should still be logged into **LON-DC1** as the **Administrator** from the prior task.
2. If **Server Manager** is closed, then re-open it now; otherwise, select the **Server Manager** icon on the taskbar.
3. In **Server Manager**, select **Tools** at the top right side of the screen, and then in the drop-down menu select **Active Directory Users and Computers.**
4. You will begin by adding members to one of the built-in security groups. In the **Active Directory Users and Computers** console tree, under **Adatum.com**, select the **Builtin** folder. This will display all the built-in security group folders that were automatically created at the time the **Adatum.com** domain was created.
5. In the detail pane on the right, double-click the **Print Operators** security group.
6. In the **Print Operators Properties** window, select the **Members** tab and then select the **Add** button.
7. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** window, in the **Enter the object names to select** field, type the following names (type all three at once with a semi-colon separating them), and then select **Check Names**:
   - **Ashlee Pickett**
   - **Juanita Cook**
   - **Morgan Brooks**
8. Select **OK** to return to the **Print Operators Properties** window.
9. In the **Print Operators Properties** window, select **OK** to return to the **Active Directory Users and Computers** window.
10. You will now create a new security group. In the console tree under **Adatum.com**, right-click on the **Research** folder, select **New,** and then select **Group**.
11. In the **New Object - Group** window, enter the following information:
    - Group name: **Manufacturing**
    - Group scope: **Universal**
    - Group type: **Security**
12. Select **OK**.
13. In the console tree under **Adatum.com**, double-click on the **Manufacturing** security group that you just added in the **Research** folder.
14. In the **Manufacturing Properties** window, in the **E-mail** box, type Manufacturing@adatum.com.
15. Select the **Members** tab, and then repeat steps 6-9 to add the following members to this group:
    - **Bernardo Rutter**
    - **Charlie Miller**
    - **Dawn Williamson**

16. Leave the **Active Directory Users and Computers** window open for the next task.

20.0.3 Task 3 - Change Group Membership to Test Synchronization

This task sets up another scenario for testing whether the sync process is working in Azure AD Connect. In this task you will change the members of a group to see if they are reflected in the cloud once the group is synced.

1. This task continues from where the previous task left off in LON-DC1. In the **Active Directory Users and Computers** window, in the console tree under **Adatum.com**, the **Research** organizational unit is still selected.

   In the detail pane on the right, double-click the **Research** security group.

2. In the **Research Properties** window, select the **Members** tab to view the members of this group.

3. You want to remove the following users from the group:

   - **Cai Chu**
   - **Shannon Booth**
   - **Tia Zecirevic**

   While you can remove each user individually, the quickest way is to remove all three at one time. Select the first user, then hold the **Ctrl** key down while selecting the other two. With all three users selected, select the **Remove** button and then select **Yes** to confirm the removal. Verify the three users have been removed, and then select **OK.**

4. Close the **Active Directory Users and Computers** window.

5. Leave LON-DC1 open as you will continue using it in the next task.

   Important: You should perform the next task immediately after completing this one so that Azure AD Connect doesn't automatically synchronize the changes that you just made to the identity objects in the previous tasks.

20.0.4 Task 4 - Force a manual synchronization

In this task, you will force a sync between Adatum's on-premises AD and Azure AD instead of waiting 30 minutes for Azure AD Connect to synchronize the identity objects. You must use PowerShell to perform a forced synchronization.

1. On LON-DC1, if the **Windows PowerShell** application is still open from the prior exercise, then **you MUST close it now**.

   Important: The reason for this step is that if Windows PowerShell was opened BEFORE the Azure AD Connect setup, the cmdlet **Start-ADSyncSyncCycle** that is used in step 3 will not be available and you will receive an error indicating that the cmdlet is not recognized when you attempt to run it. Therefore, it's recommended that at this step, you close Windows PowerShell if it's open and then restart it.

2. At this point, Windows PowerShell should NOT be open. To open it, select the **magnifying glass (Search)** icon in the taskbar, type **PowerShell** in the Search box, and then in the menu, right-click on **Windows PowerShell** (not Windows PowerShell ISE) and select **Run as administrator**.

3. In **Windows PowerShell**, run the following command to manually run a sync cycle between Adatum's on-premises AD and Azure AD. The **Delta** switch is used here so that only the updates are synchronized.

   ```
   Start-ADSyncSyncCycle -PolicyType Delta
   ```

   Note: If for any reason the Domain Controller VM was restarted after the original full synchronization run, the Microsoft Azure AD Sync service may not have restarted. If this occurred, you'll receive an error when you try to perform the forced sync above. If this occurs, you'll need to start the Microsoft Azure AD Sync service first and then perform the forced synchronization.

4. Once the synchronization process has successfully completed, minimize your PowerShell window (do not close it) and proceed to the next task. You will use PowerShell in the next task to validate some of the results of the directory synchronization.

5. Remain in LON-DC1 and proceed to the next task.

20.0.5 Task 5 - Validate the Results of Directory Synchronization

In this task, you will validate whether the changes you made earlier were synchronized from Adatum's on-premises AD to Azure AD. You will validate the changes using the Microsoft 365 admin center, and then you'll perform the same validations using Windows PowerShell. This gives you experience in validating synchronization using both the Microsoft 365 admin center GUI and PowerShell.

1. You should still be logged into LON-DC1 as the **Administrator** with a password of **Pa55w.rd.**
2. Now let's examine the synchronization results for the groups that you updated in the previous tasks. In your **Edge** browser, if tabs exists for the **Microsoft Office Home** page and the **Microsoft 365 admin center**, then proceed to the next step.

   Otherwise, enter **https://portal.office.com/** in the address bar to open the **Microsoft Office Home** page, log in as **holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) with a password of **Pa55w.rd**, and then on the **Microsoft Office Home** page, select **Admin**.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Groups**, and then select **Active groups**.
4. In the **Active groups** window, verify that the **Manufacturing** group appears in the list, and that the **Print Operators** group does NOT appear. As mentioned previously, built-in groups such as the **Print Operators** security group are not synced from the on-premises environment to Microsoft 365, even when you add members to the group as you did in the earlier task.

   Note: You may need to wait up to 10 minutes before the **Manufacturing** group appears. Continue to refresh the list until you see the group.
5. In the **Active groups** list, locate the **Manufacturing** group.

   Scroll to the right and verify the group email address was changed during directory synchronization from **manufacturing@adatum.com** to **manufacturing@M365xZZZZZZ.onmicrosoft.com**, which is the mailbox in Exchange Online.

   Scroll further to the right and verify the value in the **Sync status** indicates that it was **Synced from on-premises**. You can do this by holding your mouse over the icon that appears in the **Sync status** column to display to icon name.
6. Select the **Manufacturing** group to open the **Manufacturing** group window.
7. In the **Manufacturing** group window, note up under the Manufacturing title that it's a mail-enabled security group that contains three members. Also note the message indicating that you can only manage this group in your on-premises environment using either Active Directory users and groups (i.e. Users and Computers) or the on-premises Exchange admin center.

   The window currently displays the **General** tab. Select the **Members** tab. Note that the group has no owner (the system did not automatically assign Holly Dickson as the group owner). Verify that the three users that you added as members of the on-premises group have been synced up and are members of this cloud-based group as well. Close the **Manufacturing** group window.
8. Now let's examine this group using Windows PowerShell. If **Windows PowerShell** is already open on the taskbar, then select the PowerShell icon and proceed to the next step; otherwise, type **PowerShell** in the **Search** field on the taskbar and then right-click on the **Windows PowerShell** application and select **Run as administrator**.
9. You should begin by running the following command that connects your PowerShell session to the Microsoft Online Service:

   ```
   Connect-MsolService
   ```
10. In the **Sign in** dialog box, log in as **holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) with a password of **Pa55w.rd**.
11. Run the following command that displays a list of all the Microsoft 365 groups:

    Get-MsolGroup
12. In the list of groups that's displayed, you should verify that you can see the **Research** and **Manufacturing** groups, and that you do not see the **Print Operators** group (this is the built-in group that did not synchronize from on-premises to Microsoft 365).

13. To verify that the group membership changes that you made in your on-premises Active Directory were synced to the **Research** group in Microsoft 365, you should copy the **ObjectID** for the **Research** group to your clipboard by dragging your mouse over the ObjectId string and then pressing **Ctrl-C**.

    Then run the following command to display the members of this group. In the command, replace with the value that you copied in the prior step by pressing **Ctrl-V** to paste in the value.

    ```
    Get-MsolGroupMember -GroupObjectId <ObjectID>
    ```

14. Verify the membership of the Research group does **NOT** contain the following users that you earlier removed from the group in AD DS:

    - Cai Chu
    - Shannon Booth
    - Tai Zecirevic

15. Repeat steps 13-14 for the **Manufacturing** security group. In the **Manufacturing** group, you added the following members in AD DS, each of which you should see in the list of group members:

    - Bernardo Rutter
    - Charlie Miller
    - Dawn Williamson

16. Once you have completed the validation steps, minimize your PowerShell window (do not close it) and proceed to the next Lab.

21 End of Lab 4

22 Module 5 - Lab 5 - Exercise 1 - Deploying Microsoft 365 apps for enterprise

You have taken on the persona of Holly Dickson, Adatum's Enterprise Administrator, and you have Microsoft 365 deployed in a virtualized lab environment. In this exercise, you will perform the tasks necessary to manage a user-driven Microsoft 365 Apps for enterprise installation. Performing a user-driven Microsoft 365 Apps for enterprise installation is a two-step process: 1) configuring the user account so the user is eligible to download and install the setup file, and 2) performing the installation.

In the first two tasks in this exercise, you will verify the following conditions that affect whether a user can be blocked from downloading the Microsoft 365 Apps for enterprise suite:

- The user does not have an appropriate Office 365 license (which you will verify in Task 1).
- An admin turns off the global Office download setting that controls the downloading of mobile and desktop apps for all users (which you will verify in Task 2).

In the final task in this exercise, you will install the Microsoft 365 Apps for enterprise suite for one of Adatum's users.

22.0.1 Task 1 – Verify how licensing affects installing Microsoft 365 Apps for enterprise

In this task, Holly will test whether a user who has not been assigned an appropriate Office 365 license can download Microsoft 365 Apps for enterprise. For this test, you cannot use any of the existing users that appear in the **Active Users** list in the Microsoft 365 admin center. These users only have Microsoft 365 accounts (M365xZZZZZZ.onmicrosoft.com accounts); they do not have corresponding on-premises accounts in the adatum.com domain (which has now been changed on-premises to the xxxUPNxxx.xxxCustomDomainxxx.xxx). Without an on-premises account, you cannot log into a client VM as any of these users to install Microsoft 365 Apps for enterprise on the client machine.

Therefore, you must use one of Adatum's on-premises user accounts that has been loaded in its VM environment. For this test, you will use **Laura Atkins**. You will create an Office 365 account for Laura, but you will not assign her an Office 365 license.

You will then use the **LON-CL2** VM for installing Microsoft 365 Apps for enterprise (it's already installed on the other client machines).

1. Switch to **LON-CL2** and log in as **Administrator** with a password of **Pa55w.rd**.
2. You will begin by testing whether a user without an appropriate Office 365 license can install Microsoft 365 Apps for enterprise. For this test, you will use **Laura Atkins**. You added a Microsoft 365 user account for Laura in Lab 1, but you did not assign her an Office 365 license. For this test, you will log into Microsoft 365 on LON-CL2 as Laura.

   On LON-CL2, select the **Microsoft Edge** icon on the taskbar.
3. In **Microsoft Edge**, maximize your browser, then go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**
4. In the **Sign in** window, enter **Laura@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your tenant ID provided by your lab hosting provider) and then select **Next**.
5. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in.**
6. If a **Stay signed in?** window appears, select the **Don't show this again** check box and then select **Yes.**
7. In the **Microsoft Office Home** page for Laura, notice that no Microsoft 365 apps appear since Laura has not been assigned an Office 365 license. Select the **Install Office** drop-down arrow, and then select **Install software**.
8. This displays the **My account** window for Laura. Under the **Apps & devices** section, note the message that appears at the top of page. Laura has not been assigned an Office license that includes the Office desktop apps, so she's unable to install Microsoft 365 Apps for enterprise.

   Important: You have just verified that a user cannot download Microsoft 365 Apps for enterprise if he or she has not been assigned an appropriate Office 365 license.
9. Leave your browser and all tabs open and proceed to the next step.

22.0.2 Task 2 – Verify how the global Office download setting affects installing Microsoft 365 Apps for enterprise

Holly is now going to test whether licensed users can be prohibited from downloading Microsoft 365 Apps for enterprise if an admin such as herself turns off the global Office download setting that controls the downloading of mobile and desktop apps for all users.

1. Switch to **LON-DC1**, where you should still be logged in as the **Administrator**. You should also have your **Edge** browser open, and you should be signed into Microsoft 365 as Holly Dickson. Your browser should have tabs open for the **Microsoft Office Home** page and **Microsoft 365 admin center**.
2. To turn off the global Office download setting, select the **Microsoft 365 admin center** tab in your browser, and then if necessary, select **...Show all** in the left-hand navigation pane. Select **Settings**, and then within the group, select **Org Settings**.
3. In the **Settings** window, the **Services** tab is displayed by default. Scroll down through the list of services and select **Office software download settings.**
4. In the **Office installation options** window, scroll down to the **Apps for Windows and mobile devices** section, where the **Office (includes Skype for Business)** check box is currently selected. Select this check box so that it's blank, which turns this feature **Off**.
5. Select **Save**.

   Important: Leave the **Office installation options** window open as you will come back to it in a later step in this task.
6. Scroll back to the top of the window. Once you receive a message indicating the changes are saved, select the **X** in the upper-right corner of this window to close it.
7. You should now test whether turning off this global download setting affects a **licensed** user from installing Microsoft 365 Apps for enterprise. In this case, you are going to use **Alan Yoo**, who you also added in Lab 1; however, unlike Laura Atkins, you assigned Alan an Office 365 E5 license.
8. Switch to **LON-CL2**.

9. In LON-CL2, you should still be logged in as Laura Atkins from the prior task. You must first log out of Microsoft Office as Laura, so select the circle with the **LA** initials in the upper right corner of the screen. In the **My accounts** window, select **Sign out**.

   Important: As a best practice to avoid any confusion when logging out as one user and logging in as another, close all other tabs that are open in your Edge browser except for this **Sign out** tab.

10. In the **Sign out** tab, go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**

11. You are now going to sign into Microsoft 365 as **Alan Yoo**. In the **Pick an account** window, select **Use another account**. In the **Sign in** window, enter **Alan@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your tenant ID provided by your lab hosting provider) and then select **Next**.

12. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in.**

13. If a **Get your work done with Office 365** window appears, select the X in the upper right hand corner to close it.

14. In the **Microsoft Office Home** page for Alan, notice that the Microsoft 365 apps now appear because Alan has been assigned an Office 365 license. If an **Install software** box appears, select the **Got it!** button.

15. Select the **Install Office** drop-down arrow, and then in the drop-down menu, select **Other install options**.

16. In the **My account** window, under the **Office apps & devices** section, select **View apps & devices**.

17. In the **Apps & devices** window, under the **Office** section at the top of the page, a message is displayed indicating the admin has turned off Office installs.

    Important: You have just verified that a licensed user is unable to download Microsoft 365 Apps for enterprise if the global Office download setting has been turned Off.

18. At this point Holly wants to turn the global Office download setting back On so that Alan can download Microsoft 365 Apps for enterprise.

    To do this, you must switch back to **LON-DC1**. The **Office installation options** window should still be open in your browser from when you earlier turned Off the Global Office download option.

    In the **Office installation options** window, under the **Apps for Windows and mobile devices** section, the **Office (includes Skype for Business)** check box is currently blank. Select this check box so that it displays a check mark, which now turns this feature back On.

19. Select **Save**.

20. Once you receive a message indicating the changes are saved, select the **X** in the upper-right corner of this window to close it.

21. Now that this global Office download option is turned back On, you should see if it affects Alan's ability to download Microsoft 365 Apps for enterprise.

    To do this, you must switch back to **LON-CL2**.

22. In LON-CL2, Alan's Edge browser should still be open, and the **Apps and devices** page should be displayed along with the error message that indicated your admin has turned off Office installs. Since you just turned this option back On, you need to refresh this page to see how it affects Alan's ability to download Microsoft 365 Apps for enterprise.

    Select the **Refresh icon** that appears to the left of the address bar at the top of your browser.

23. In the **My account** window that appears, under the **Office apps & devices** section, the **Install Office** button now appears along with a message indicating you can install Office on up to 5 PCs or Macs, 5 tablets, and 5 smartphones.

    Important: You have just verified that a user with an Office license is able to download Microsoft 365 Apps for enterprise if the global Office download setting is turned On.

24. Leave this page open on LON-CL2 and continue to the next task to perform the user-driven installation for Alan Yoo.

22.0.3 Task 3 – Perform a User-Driven Installation of Microsoft 365 Apps for enterprise

In the prior task, you logged into Alan Yoo's client PC, and you verified that a licensed user could download Microsoft 365 Apps for enterprise if he or she was assigned an Office 365 license and the global Office download setting was turned On. In this task, you will continue the process by having Alan Yoo perform a user-driven installation of the Microsoft 365 Apps for enterprise suite from the Microsoft 365 portal.

1. On LON-CL2, you should still be logged in as Alan Yoo.
2. You should still be in Alan's **My account** window since this is where you left off at the end of the prior task. Under the **Office apps & devices** section, the **Install Office** button now appears since Alan is assigned an Office 365 E5 license and the global Office download setting is turned On.

   Important: Selecting this **Install Office** button will install the 64 bit, English version of Microsoft 365 Apps for enterprise. However, if you want to install a different language or version, then select **View apps & devices**, which opens the **Apps & devices** page; this enables you to select a different language and version of Microsoft 365 Apps for enterprise to install.

   Since Alan wants to install the 64-bit English version of Microsoft 365 Apps for enterprise, select the **Install Office** button.
3. In the **Just a few more steps** window that appears, select **Close**. This will initiate the downloading of the 64-bit Microsoft 365 Apps for enterprise installation wizard (**OfficeSetup.exe**).
4. In the notification bar that appears at the bottom of the page, once the **OfficeSetup.exe** file is downloaded, select **Open file**. This will initiate the installation wizard.
5. In the **Do you want to allow this app to make changes to your device?** dialog box that appears, select **Yes**. If you are prompted to enter a username and password, enter **adatum\administrator** in the **username** box and **Pa55w.rd** in the **Password** box.
6. You may receive a dialog box that displays a warning message indicating that it may be expensive to continue downloading. Select **OK.**

   Important: This window may appear behind the Office window that displays the message: **We're getting things ready.** If so, move the Office window to the side so that you can respond to the warning message. The Office install will NOT proceed until you select **OK** on the warning message (the Office window will just keep displaying the **We're getting things ready** message, but it won't actually do anything).
7. The installation may take several minutes to complete. The installation window will close once the installation is complete.
8. To verify Alan Yoo's Microsoft 365 Apps for enterprise installation, select the **Start** icon in the lower-left corner of the taskbar. Below the **Recently added** section (at the top of the **Start** menu) select **Expand** to display all the Microsoft 365 Apps for enterprise that were just installed. This should include Word, PowerPoint, OneNote, Outlook, Publisher, Access, Skype for Business, and Excel.
9. In the **Start** menu, select **Word**.
10. On the **Hello Alan, welcome to Office** window that appears, select the **X** in the upper-right hand corner to close the window.
11. On the **Accept the license agreement** window, select **Accept**.
12. On the **Your privacy option** window, select **Close**.
13. Verify that Word is functioning properly by opening a blank Word document, entering some text, and saving the document to the **Documents** folder.
14. Close Word.
15. Leave your browser open and proceed to the next lab.

23 End of Lab 5

24 Module 6 - Lab 6 - Exercise 1 - Managing Exchange Online recipients

As part of its Microsoft 365 deployment, Adatum wants to implement Exchange Online. As part of Adatum's pilot project, Holly Dickson, Adatum's Enterprise Admin, wants to investigate three key features related to mail flow recipients within Exchange Online - user mailboxes, groups, and contacts.

Holly will begin by creating user accounts and mailboxes in Exchange Online. She will then create two types of groups within Exchange Online. The first will be a distribution list of email recipients, which is used to create a one-stop email list for contacting users simultaneously rather than having to email each recipient individually. The second type of group is a Microsoft 365 group.

One of the key features of Exchange Online is the ability to maintain different types of contacts in the Exchange Admin Center. Holly will complete this exercise by implementing mail contacts and mail users.

24.0.1 Task 1 – Manage Recipients

As you continue in your role as Holly Dickson, you are ready to review the steps involved in creating and managing mail flow recipients in Exchange Online.

1. Switch to LON-CL1, where you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. You should still have **Microsoft Edge** open and the **Microsoft 365 admin center** open from the prior lab. If so, proceed to the next step; otherwise, open Edge, navigate to **https://portal.office.com/**, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and **Pa55w.rd**, and then in the **Microsoft Office Home** page, select **Admin** to open the Microsoft 365 admin center.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all** (if necessary), then scroll down to **Admin centers** and select **Exchange**. This will open the **Exchange admin center** for Exchange Online.
4. In the **Exchange admin center,** select **recipients** in the left-hand navigation pane.
5. In the **recipients** view, the **mailboxes** tab appears by default (see the tabs at the top of the page). The mailboxes that appear in this view include all the user accounts that were pre-created in your tenant by the lab hosting provider, along with mailboxes for users that you created in Lab 2 that were assigned an Office 365 license (Holly, Ada Russell, Alan Yoo, Catherine Richard, and Tameka Reed). Note the users that you created in the earlier lab that were not assigned a license (such as Adam Hobbs) do not have an Exchange Online mailbox.

   Select the mailbox for **Joni Sherman** by double-clicking on her **DISPLAY NAME.** This will open the **Edit Mailbox** window with Joni's data prefilled. By default, the window displays the **general** tab (the tabs appear in the left-hand pane).
6. The **general** tab in the left-hand navigation pane is displayed by default. At the bottom of the **general** tab, select **More options**.
7. Under **Custom attributes**, select the **pencil (edit)** icon.
8. This opens the **Custom attributes** window for Joni. You can enter up to 15 attributes. You will not be entering any attributes in this lab exercise, but it's important that you know this feature is available. Select **Cancel**.

   Note: Custom attributes are properties your company can use for specific mailbox identification, such as a cost center number for the mailbox or other information such as an HR personnel number.
9. In addition to the **general** tab, the left-hand pane of the **Edit Mailbox** window includes several other tabs that enable you to enter additional information pertaining to this specific mailbox. While you will not enter any of this optional information for the purposes of this lab, take a few minutes now and select the following tabs to see what information can be captured:
   - **contact information.** This tab enables you to add personal information such as Street, City or Mobile number for the user.

- **organization.** This tab enables you to add company-specific information such as Title or Department for the user.
- **mailbox features.** This tab enables the admin to assign specific policies to the user. These policies range from the sharing policy to the address book policy. This option also covers device usage and connectivity.
- **member of.** This tab displays the Distribution groups that include this user.

10. On the left-hand pane select **mailbox delegation.** This option allows the admin to assign a user to this mailbox's Send As, Send on Behalf, or Full Access permissions. This option is commonly used if you want another user to be able to send messages from this mailbox.

    Scroll down on this **mailbox delegation** window and select the plus (+) sign under the **Full Access** section.

11. In the **Select Full Access** window select **Holly Dickson**, select the **add->** button, and then select **OK.**

    Note: After about an hour Holly Dickson will be able to access Joni's mailbox without needing a password.

12. On Joni Sherman's **Edit Mailbox** window, select **Save**, and then select **OK** once the changes are saved.
13. Leave your browser and all the tabs open for the next task.

24.0.2 Task 2 – Manage Groups

In this task you will create two types of groups within Exchange Online. The first is a distribution list of email recipients, which is used to create a one-stop email list for contacting users simultaneously rather than having to email each recipient individually. The second type of group is an Office 365 group.

1. You should still be in LON-CL1 and your browser should still be open to the **Exchange admin center** from the prior task, where it should still be displaying **recipients** from the left-hand navigation pane. In the prior task, you worked with user accounts using the **mailboxes** tab. In this task, you will be creating groups, so select the **groups** tab at the top of the **recipients**' page.

    Note: You should see the Inside Sales and Manufacturing groups that you created in earlier labs.

2. Select the drop-down arrow next to the **New Microsoft 365 group** button. In the drop-down menu, select **Distribution list**.
3. In the **new distribution list** window that appears, enter the following information:
    - Display Name: **Sales Department**
    - Alias: **SalesDept**
    - Email Address: tab into the field and the **SalesDept** alias will appear. In the domain field to the right of it, select the drop-down arrow and select **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider).
    - Owners: Since you are logged into the EAC using Holly Dickson, her account is displayed as the default Owner. However, Holly wants Alex Wilber to co-own the group, so select the **plus (+)** sign under the **Owners** section, and in the **Select Owner** window, select **Alex Wilber**, select the **add->** button, and then select **OK**.
    - Members: select the plus (+) sign under the **Members** section, and in the **Select Members** window, select **Allan Deyoung**. Then hold down the **Ctrl** key and select **Diego Siciliani** and **Lynne Robbins**. This will select all three users at once, at which point you should select the **add->** button and then select **OK**.
4. Select **Save** and then select **OK** once the changes are saved successfully.
5. Select the **+New Office 365 group** button (not the drop-down arrow to the right of it, but the button itself).
6. In the **Create a group** window that appears, enter the following information:
    - Group name: **Dynamics CRM Project Team**
    - Group email address: **DynCRM**

- Group email address domain: In the domain field to the right of the **DynCRM** alias, select the drop-down arrow and select **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
- Privacy: **Public – Anyone can see content**
- Owners: Leave as **Holly**
- Language: Leave as **English**
- Description: **Group of all company employees working on the Microsoft Dynamics CRM project.**
- Subscribe new members: leave this check box selected so that members get conversations and calendar events sent to their Inboxes

7. Select **Save** and then select **OK** once the changes are saved successfully.
8. In the **Dynamics CRM Project Team** window that appears, you will now perform maintenance on this existing group. The **ownership** tab in the left-hand pane is displayed by default. Under **Owners**, select the **plus (+)** sign, and in the **Select Members** window, select **Nestor Wilke**, select the **add->** button, and then select **OK**.
9. In the left-hand pane, select **membership**.
10. Under **Members**, select the **plus (+)** sign, and in the **Select Members** window, select **Isaiah Langer**. Then hold down the **Ctrl** key and select **Joni Sherman**, and **Patti Fernandez**. This process will select all three users. Select the **add->** button and then select **OK.**
11. Select **Save** and then select **OK** once the changes are saved successfully.
12. Leave your browser and all the tabs open for the next task.

24.0.3 Task 3 – Manage Resources

A room mailbox is a resource mailbox that is assigned to a physical location, such as a conference room, an auditorium, or a training room. Users can easily reserve these rooms by including room mailboxes in their meeting requests. Adatum's CTO wants to test this feature using the company's most popular conference room, and he has asked Holly to configure this resource.

1. You should still be in LON-CL1 and your browser should still be open to the **Exchange admin center** from the prior task, where it should still be displaying **recipients** from the left-hand navigation pane, and on the **recipients** page, it should be displaying the **groups** tab. In the prior tasks you managed mailbox and group recipients; in this task, you will manage resource recipients.

   On the **recipients** page, select the **resources** tab at the top of the page.
2. In the menu bar that appears over the list of resources, select the **plus (+)** sign and then in the drop-down menu, select **Room mailbox.**

   Note: This selection is designed for administrators to set up a meeting location to be used for booking purposes. When scheduling meetings, you will be able to select the room from the Global Address List (GAL).
3. In the **new room mailbox** window that appears, enter the following information:
   - Room name: **Conference Room 1**
   - Email address: **Con1**
   - Email address domain: In the domain field to the right of the **Con1** alias, select the drop-down arrow and select **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
   - Location: The room is in Building 5, Room 2011, so enter **5/2011**
   - Phone: **425-555-2011**
   - Capacity: **15**
4. Select **Save** and then select **OK** once the changes are successfully saved.

5. **Conference Room 1** now appears in the list of resources. You must now edit the booking properties for this resource. Since Conference Room 1 is the only resource in the list, it's already selected by default; therefore, select the **Edit** (pencil) icon on the menu bar.
6. In the **Conference Room 1** window that appears, select **booking options** in the left-hand pane.
7. Select the **Allow scheduling only during working hours** check box.
8. In the **Maximum booking lead time (days)** field, change the value from **180** days to **60** days.

   Note: The standard duration of 180 days can be too long for scheduling out most meetings. As a best practice, organizations should establish a company standard so that events do not over-book locations.
9. In the **Maximum duration (hours)** field, change the value from **24.0** hours to **120** hours (this is five days, or one work week).
10. In the left-hand navigation pane, select **booking delegates**.
11. Select the **Select delegates who can accept or decline booking requests** option.

    Note: This option allows a user to filter booking requests.
12. Under **Delegates**, select the **plus (+)** sign. In the **Select Delegates** window, select **Holly Dickson** and then hold down the **Ctrl** key and select and **Nestor Wilke**. This will select both users at once; then select the **add->** button and select **OK.**
13. Select **Save** and then select **OK** once the changes are successfully saved.
14. Leave your browser and all the tabs open for the next task.

24.0.4 Task 4 – Manage Contacts

One of the key features of Exchange Online is the ability to maintain different types of contacts in the Exchange Admin Center. In this task, you will be introduced to mail contacts and mail users.

1. You should still be in LON-CL1 and your browser should still be open to the **Exchange admin center** from the prior task, where it should still be displaying **recipients** from the left-hand navigation pane. In this list of recipient tabs across the top of the screen, select **contacts.**
2. In the menu bar that appears over the list of contacts, select the **plus (+)** sign, and in the menu that appears, select **Mail contact.**

   Note: This option enables external people from outside your organization to be added to your Exchange Online distribution lists.
3. In the **new mail contact** window that appears, enter the following information.
   - First name: **Bao**
   - Initials: leave blank
   - Last Name: **Chu**
   - Display Name: tab into the field and **Bao Chu** is automatically displayed
   - Alias: **Hai**
   - External Email Address: **Hai@fabrikam.com**
4. Select **Save** and then select **OK** once the changes are successfully saved. Hai should now appear in the list of contacts as a **Mail contact**.
5. On the menu bar above the contacts list, select the **plus (+)** sign to add another contact. In the drop-down menu, select **Mail user.**

   Note: This option is for individuals who need to use the company domain even though they are not a full-time employee (for example: contractors, advisors, and selective temporary staff). This option will forward email to the individual's external email when mail is sent to the contact's internal company account.

   WARNING: A Mail User does not need a license to access SharePoint Online; the user simply needs to be given access to it.
6. In the **new mail user** window that appears, enter the following information:

- First name: **Albert**
- Initials: leave blank
- Last Name: **Eksteen**
- Display Name: tab into the field and **Albert Eksteen** is automatically displayed
- Alias: **Albert**
- External email address: **Albert@fabrikam.com**
- User ID: **v-Albert** (this is the user's alias for his internal Adatum account)
- User ID domain: in the domain field to the right of the User ID, select the drop-down arrow and select **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
- New password: **Pa55w.rd**
- Confirm Password: **Pa55w.rd**

7. Select **Save** and then select **OK** once the changes are successfully saved. Bill should now appear in the list of contacts as a **Mail user**.
8. In your Edge browser session, leave all the tabs open, including the Exchange admin center; these will be used in the next lab exercise.

25 Proceed to Lab 6 - Exercise 2

26 Module 6 - Lab 6 - Exercise 2 - Configuring Exchange Online permissions

In this exercise you will continue in your role as Holly Dickson, Adatum's Enterprise Administrator. Holly has been tasked with managing admin roles and permission policies for Adatum. The CTO has asked Holly to create a new management role group that allows an administrator to remotely access a mailbox without having the password.

In the prior lab exercise, you maintained Exchange Online recipients from the Exchange Admin Center. In this exercise, you will use Windows PowerShell to create a new Exchange role, assign members to it, and create a new role assignment policy. This will provide you with experience using both the online admin center and PowerShell to manage Exchange recipients and permissions.

26.0.1 Task 1 Create a new admin role and assign a user to it

In this task you will configure Exchange admin roles through Windows PowerShell. Creating a new role such as this is useful when you want to limit the amount of control given to a person who will only be in an administrative role temporarily.

1. You should still be logged into **LON-CL1** as the **Administrator** account with a password of **Pa55w.rd**.
2. Windows PowerShell should be open from an earlier lab exercise. However, if you closed it, then re-open an elevated instance of it (Run as administrator) now.
3. In the **Windows PowerShell** window, at the command prompt type the following command and then press Enter to set the execution policy to remote signed, which requires that all scripts and configuration files downloaded from the Internet are signed by a trusted publisher.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   If you are prompted to verify that you want to change the execution policy, enter **A** to select [**A**] **Yes to All.**
4. At the command prompt, enter the following command and then press Enter to install the Exchange Online Management Module into Windows PowerShell.

   ```
   Install-Module -Name ExchangeOnlineManagement
   ```

   If you are prompted to verify that you want to install the module from an untrusted repository, enter **A** to select [**A**] **Yes to All.**

5. At the command prompt, enter the following command and then press Enter to prompt you for the sign-in credentials of the user who will be signing into Exchange Online. For each subsequent command that is run, these credentials will be verified to determine if the user has the permissions necessary to make the change.

```
$UserCredential = Get-Credential
```

6. In the **Windows PowerShell credential request** window that appears, enter the credentials of Adatum's MOD Administrator. Enter **admin@M365xZZZZZZ.onmicrosoft.com** in the **User name** field (where ZZZZZZ is your tenant ID), enter the tenant password provided by your lab hosting partner in the **Password** field, and then select **OK**.

7. At the command prompt, enter the following command and then press Enter to connect you to Exchange Online and sign in automatically with your stored credentials.

```
Connect-ExchangeOnline -Credential $UserCredential -ShowProgress $true
```

8. At the command prompt, enter the following command and then press Enter. This command is specific to this task. Normally running the following commands would result in an unauthorized access error; however, this command enables you to run them. Note: This command is only for Exchange Online use.

```
Enable-OrganizationCustomization
```

9. At the command prompt, enter the following command and then press Enter to create a new role group called **BranchOfficeAdmins**, with the following roles assigned to it: **Mail Recipients**, **Distribution Groups**, **Move Mailboxes**, **Mail Recipient Creation**.

```
New-RoleGroup -Name BranchOfficeAdmins -roles "Mail Recipients", "Distribution Groups", "Move Mai
```

Note: This command may take a few minutes to complete.

10. At the command prompt, enter the following command and then press Enter to add Nestor Wilke to the Branch Office Admins role group:

```
Add-RoleGroupMember "BranchOfficeAdmins" -Member 'Nestor Wilke'
```

11. At the command prompt, enter the following command and then press Enter to retrieve all members associated to Branch office admins role group (which, at this point, is only Nestor Wilke):

```
Get-RoleGroupMember "BranchOfficeAdmins"
```

12. Minimize the Windows PowerShell window.

13. You will now verify the changes that you made in PowerShell are visible in the Exchange admin center. Your Edge browser should be open from the prior task, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

    If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.

14. In the **Exchange admin center**, in the left-hand navigation pane, select **permissions**.

15. On the **permissions** page, the **admin roles** tab is displayed by default. The **BranchOfficeAdmins** role group should appear in the list of admin roles. Select **BranchOfficeAdmins**.

16. The detail pane for the **BranchOfficeAdmins** role group should appear to the right of the list. This detail pane displays all the roles assigned to this role group, as well as Nestor Wilke, who is the only member.

17. Leave your browser and all tabs open.

26.0.2 Task 2: Create a new role assignment policy

Exchange Online comes with a default user role policy titled **Default Role Assignment Policy**. This policy grand end users the permission to set their options in Outlook on the web and perform other self-administration tasks.

Holly Dickson wants to add an additional role assignment policy and set it as the default policy for Adatum. In this task, she will use PowerShell to create the policy and set it as Adatum's new default policy.

1. At the end of the prior task, you were in **LON-CL1** in the **Exchange admin center**, and you displayed the **permissions** tab. On the **permissions** page, you had selected the **admin roles** tab.

   On the **permissions** page, you should now select **user roles**. Note that there is only one role, the **Default Role Assignment Policy**.

   In this task, you are going to create a new role assignment policy, but instead of doing it through the Exchange admin center, you will do it through Windows PowerShell. Therefore, minimize your Edge browser.

2. In the prior task, you minimized the Windows PowerShell console once you were done with PowerShell. Now that you will be using PowerShell again, select the **Windows PowerShell** icon on the taskbar.

3. In the **Windows PowerShell** console, at the command prompt, enter the following command and then press Enter to create a new user role policy titled **Limited Mailbox Configuration**, with the following roles assigned to it: **MyBaseOptions**, **MyAddressInformation**, and **MyDisplayName**.

   ```
   New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles MyBaseOptions,MyAddressInformatio
   ```

4. At the command prompt, enter the following command and then press Enter to change the default role assignment policy for new mailboxes. This command will set the **"Limited Mailbox Configuration"** policy to be the new default Role assignment policy.

   ```
   Set-RoleAssignmentPolicy "Limited Mailbox Configuration" -IsDefault
   ```

   When prompted to confirm whether you set the Limited Mailbox Configuration policy as the default Role Assignment Policy, enter **A** to select **[A] Yes to All.**

5. Minimize the **Windows Powershell** console.

6. Select the **Edge** browser icon on the taskbar, and then select the **Exchange admin center** tab.

7. In the **Exchange admin center**, you should still be on the **permissions** page and displaying the **user roles** tab. In the menu bar that appears above the list of user roles, select the **Refresh** icon. You should now see the new **Limited Mailbox Configuration** role assignment policy that you created in PowerShell.

8. Leave your browser and all tabs open and proceed to the next lab.

Results: After completing this exercise, you will have configured delegated administration of your Exchange Online organization.

27 End of Lab 6

28 Module 7 - Lab 7 - Exercise 1 - Configuring message transport settings

In this exercise, you will take on the persona of Holly Dickson, Adatum's Enterprise Administrator. As part of her pilot project for Adatum's Exchange deployment, Holly wants to begin by creating custom send and receive connectors in her Exchange Online deployment using the Microsoft 365 Exchange admin center. Exchange uses connectors to enable incoming and outgoing mail flow in Exchange Online and between services in the transport pipeline.

You will then create a series of mail flow rules that are designed to protect Adatum's messaging environment. You will first create a mail flow rule that adds a disclaimer message to each received email; the message will indicate that you must delete the message if you are not the intended recipient. You will then create a second rule in which any email received that was intended for Megan Bowen must be forwarded automatically to the MOD Administrator for approval first. Finally, if the Development teams sends or receives email, then journal reports will be sent to a specific web address.

28.0.1 Task 1 - Create a custom send and receive connector to enforce TLS

In this task you will create two connectors to enforce Transport Layer Security (TLS) with Trey Research, one of Adatum's most important partners who deals in top-secret government information that must be encrypted within email messages. One connector will be a send (outbound) connector from Adatum to Trey Research. The second connector will be a receive (inbound) connector from Trey Research to Adatum.

Important: Connectors help control the flow of email messages to and from your Microsoft 365 organization. While most organizations do not require connectors, there are certain scenarios that require them. For Adatum, it frequently exchanges top-secret information with Trey Research. As such, Adatum wants to apply security restrictions by using TLS to encrypt sensitive information.

1. You should still be logged into **LON-CL1** as the **Administrator** account with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior lab, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **mail flow**.
4. On the **mail flow** page, the **rules** tab is displayed by default. In the list of tabs across the top of the page, select **connectors**.
5. On the **connectors** page, you want to add a new send connector. Select the **plus sign icon (+)** that appears on the menu bar above the list of connectors.
6. On the **Select your mail flow scenario** page, select the drop-down arrow in the **From** box and then select **Office 365 ** from the menu.

   In the **To** box, select the drop-down arrow, select **Partner organization**, and then Select **Next**.
7. On the **New connector** page, enter **Trey Research Outgoing** in the **Name** box and then select **Next**.
8. On the **When do you want to use this connector?** page, select the **Only when email messages are sent to these domains** option, and then select the **plus (+) sign** icon to add domains.
9. On the **add domain** page, enter **treyresearch.net**, select **OK**, and then select **Next**.
10. On the **How do you want to route email messages?** page, select the **Use the MX record associated with the partner's domain** option and then select **Next**.
11. On the **How should Office 365 connect to your partner organization's email server?** page, select the **Always use Transport Layer Security (TLS) to secure the connection** check box, select the **Issued by a trusted certificate authority (CA)** option, and then select **Next.**
12. On the **Confirm your settings** page, select **Next**.
13. On the **Validate this connector** page, select the **plus (+) sign** icon to add an email address for the partner domain, which in this case is **treyresearch.net**.
14. On the **add email** page, enter **postmaster@treyresearch.net** in the email address field, select **OK**, and then select **OK** once the information is successfully saved.
15. On the **Validate this connector** page, select **Validate**.

    Wait while validation completes and then select **Close**.
16. On the **Validation Result** page, select **Save**. Note the status of the **Send test email** task is **Failed**.
17. In the **Warning** window, select **Yes** to still save the connector even though the validation failed, and then select **OK** once the connector is successfully saved.

    Note: Validation of mail flow to this connector will fail because the connector is for a fictitious organization that does not exist. This is expected behavior for this lab.
18. You just added a send (outbound) connector from Adatum to Trey Research. You will now create a receive (inbound) connector from Trey Research to Adatum. In the **Exchange admin center**, on the **connectors** tab, select the **plus sign (+)** icon on the menu bar to add another connector.
19. On the **Select your mail flow scenario** page, in the **From** box, select **Partner organization**.

    In the **To** box, select **Office 365** and then select **Next**.
20. In he **New connector** page, enter **Trey Research Incoming** in the **Name** field and then select **Next**.
21. In the **How do you want to identify the partner organization?** page, select the **Use the sender's domain** option and then select **Next**.

22. In the **What sender domain do you want to use to identify your partner?** page, select the **plus (+) sign** icon to add domains.
23. On the **add domain** page, enter **treyresearch.net**, select **OK**, and then select **Next**.
24. On the **What security restrictions do you want to apply?** page, select the **Reject email messages if they aren't sent over TLS** check box and then select **Next**.
25. On the **Confirm your settings** page, select **Save**, and then select **OK** once the information is successfully saved.
26. On the **Connectors** page, you should now see the send (outbound) and receive (inbound) connectors that you just created.
27. Leave your browser and all tabs open for the next task.

28.0.2 Task 2: Create transport rules

In the next few tasks, you will create a series of mail flow rules that are designed to protect Adatum's messaging environment. In this task, you will create a mail flow rule that adds a disclaimer message to each received email; the message will indicate that you must delete the message if you are not the intended recipient. You will then create a second rule in which any email received that was intended for Megan Bowen must be forwarded automatically to the MOD Administrator for approval first.

1. You should still be logged into **LON-CL1** as the **Administrator** account with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior task, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.
3. In the **Exchange admin center**, the **mail flow** tab in the left-hand navigation pane should still be selected from the prior task, and on this page, the **connectors** tab should be displayed. Since you want to create a message transport rule, select the **rules** tab at the top of the page.
4. You will begin by creating a rule that adds a disclaimer message to each received email. On the **rules** tab, select the **plus (+) sign** icon on the menu bar. In the menu that appears, select **Apply disclaimers**.
5. In the **new rule** window, enter the following information:
   - In the **Name** field, enter **A. Datum Disclaimer**
   - In the **Apply this rule if** box, select **The recipient is located**. This opens a **Select sender location** window. Select **Inside the organization** and then Select **OK**.
   - To the right of the **Do the following** field, select the **Enter text** hyperlink. In the **specify disclaimer text** window, enter the following message in the text field and then select **OK**: **If you are not the intended recipient of this message, you must delete it.**
   - To the right of the **Do the following** field and below the disclaimer that you just entered, select the **Select one** hyperlink. On the **specity fallback action** window, you must select an action to be performed if the disclaimer cannot be inserted. In this case, select **Wrap** and then Select **OK**.
   - Under **Properties of this rule**, verify the **Audit this rule with severity level** check box is selected. In the corresponding field, select the drop-down arrow and then select a severity level of **Medium**.
   - In the **Choose a mode for this rule** option, select **Enforce**.
6. In the **new rule** window, select **Save**.
7. If the **Warning** window appears, select **Yes**.
8. You will now create a second mail flow rule that automatically forwards to the MOD Administrator any email intended for Megan Bowen; the MOD Administrator must approve the email before it can be forwarded to Megan.

   On the **rules** tab, select the **plus (+) sign** icon on the menu bar. In the menu that appears, select **Send messages to a moderator**.
9. In the **new rule** window, enter the following information:
   - In the **Name** field, enter **Messages that must be moderated**
   - In the **Apply the rule if** box, select **The recipient is a member of**.
   - In the **Select Members** window, select **Megan Bowen**, select **add**, and then select **OK**.

- In the **Do the following** box, select **Forward the message for approval to**.
- In the **Select Members** window, select **MOD Administrator**, select **add**, and then select **OK**.
- Under **Properties of this rule**, verify the **Audit this rule with severity level** check box is selected. In the corresponding field, select the drop-down arrow and then select a severity level of **Low**.
- In the **Choose a mode for this rule** option, select **Enforce**.

10. In the **new rule** window, select **Save**.
11. Leave your browser and all tabs open for the next task.

28.0.3 Task 3: Validate the new transport rules

In this task, you will test the new transport rules that you created in the prior task. You will send an email from Patti Fernandez to Megan Bowen, which should trigger the two message transport rules. You will then verify the Disclaimer message is added to the message, and that the message is forwarded to the MOD Administrator for approval.

1. Switch to **LON-CL2**. You should still be logged in as the **Administrator**.
2. If **Microsoft Edge** is open, you should still be logged into Microsoft 365 as Alan Yoo from an earlier lab. Log out as Alan, then close all tabs except for the **Sign out** tab. Then close your Edge browser session.

   Once Edge is closed, then the **Edge** icon on the taskbar to open a new browser session.
3. In **Microsoft Edge**, open a new tab and then enter the following URL in the address bar: **https://Outlook.office365.com**
4. In the **Pick an account** window, select **Use another account**. In the **Sign in** window, enter **PattiF@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is then tenant ID provided by your lab hosting provider) and select **Next**. In the **Enter password** window, enter the password provided by your lab hosting provider for the tenant admin account and then select **Sign in**.
5. In **Outlook on the web**, close the **Welcome** window.
6. In **Outlook on the web**, select the **New message** button.
7. In the email form, in the **To** field, enter **Megan**. This will display a list of users whose first name starts with Megan. Select **Megan Bowen**.
8. In the **Subject** field, enter **Message transport tests**.
9. In the message body, enter **Disclaimer message test and moderator approval test** and then select **Send**.
10. You will now sign out as Patti Fernandez and then sign into Outlook on the web as the MOD Administrator. Select the picture of Patti in the upper right corner of the screen, and in the **My account** window that appears, select **Sign out**.
11. Once you are signed out of **Outlook on the web**, enter the following URL in the address bar: **https://Outlook.office365.com**
12. In the **Pick an account** window, select **Use another account**. In the **Sign in** window, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is then tenant ID provided by your lab hosting provider) and select **Next**. In the **Enter password** window, enter the password provided by your lab hosting provider for the tenant admin account and then select **Sign in**.
13. In **Outlook on the web**, close the **Welcome** window.
14. In **Outlook on the web**, check the MOD Administrator's **Inbox**. If you see the message from Patti to Megan, open the message and verify the disclaimer message was added to the body of the email.

    However, if the email is not in the MOD Admin's Inbox, check the **Junk** folder. If the email is not there, then sign out of Outlook on the web as the MOD Admin, repeat steps 11-12 to sign into Outlook on the web as **Megan Bowen** (where the username will be **MeganB@M365xZZZZZZ.onmicrosoft.com** and the password provided by your lab hosting provider for the tenant admin account.

    If the email from Patti is in Megan's Inbox, then verify the disclaimer message was added. However, the fact that this email is in Megan's Inbox indicates the second message transport rule that you created has not completely propagated through Microsoft 365. Sometimes it takes several hours for transport rules

to fully propagate. If this is the case, switch back to LON-CL1 and verify the **Messages that must be moderated** rule is set up properly. If everything looks OK, then wait an hour or so, switch back to LON-CL2, and then repeat this task (sign in as Patti, create the email, then sign back in as the MOD Admin to verify the email).

15. On LON-CL2, sign out of Outlook as the MOD Administrator, and then close your Edge browser session.

28.0.4 Task 4 - Create a journal rule for members of the Manufacturing Group

In this task, you will create a transport rule whereby, if the Manufacturing group sends or receives email, then journal reports will be sent to a specific web address.

1. Switch to **LON-CL1**, where you should still be logged in as the **Administrator**.
2. The Edge browser should be open from the prior lab, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **compliance management**.
4. On the **compliance management** page, the **In-place eDiscovery & Hold** tab is displayed by default. In the list of tabs across the top of the page, select **journal rules**.
5. On the **journal rules** page, the following line appears above the menu bar: **Send undeliverable journal reports to Select address**. The **Select address** portion of this message is hyper-linked. Select **Select address**.
6. In the **non-delivery reports** window that appears, select **Browse**. In the list of users that appears, select **MOD Administrator**, select **OK**, and then back on the **non-delivery reports** window, select **Save**.
7. In the **Warning** window, select **OK**.
8. On the **journal rules** page, select the **plus (+) sign** icon on the menu bar to add a new journal rule.
9. In the **new journal rule** window, in the **Send journal reports to** field, enter **journal@treyresearch.net**.
10. In the **Name** field, enter **Manufacturing Group Messages**.
11. In the **If the message is sent to or received from** field, select **A specific user or group**, and then in the list users and groups that appears, select **Manufacturing**, select **add**, and then select **OK**.
12. In the **Journal the following messages** field, select **All messages**, and then select **Save**.
13. Leave your browser and all tabs open for the next task.

28.0.5 Task 5 - Track internal and external message delivery

1. You should still be logged into LON-CL1 as the **Administrator**.
2. The Edge browser should be open from the prior task, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **mail flow**.
4. On the **mail flow** page, the **rules** tab is displayed by default. In the list of tabs across the top of the page, select **message trace**.
5. On the **message trace** page, note the banner at the top of the page indicating that a new and improved Message Trace has been added in the Security & Compliance center. Select **Go to the new Message Trace now**. This will open a new tab in your Edge browser for the **Security & Compliance Center**.
6. In the **Security & Compliance Center**, in the left-hand navigation pane, select **Mail flow** and then select **Message trace**.

7. In the **message trace** window, note how it provides categories for existing search queries. Select each group to expand it to view the pre-defined queries for that group.
8. Once you have finished reviewing the pre-defined queries, select the **+Start a trace** button.
9. In the **New message trace** window, review the search options and then select **Search**.
10. In the **Message trace search results** window, select the message sent from Patti Fernandez to Megan Bowen.
11. In the **Message trace details** window, review the information in the message. Select the arrow in the **Message events** section to expand it. In the **Event** column, note the **Transport rule** event, which applied the disclaimer transport rule.
12. If the **Message transport tests** transport rule was applied, note the event that sent the message to the MOD Administrator.
13. Select **Close**.
14. In the **Message trace search results** window, select **Close**.
15. Close the **New message trace** window.
16. Close the **Message trace - Security & Compliance Center** tab in your browser. Leave the remaining tabs open for the next lab exercise.

Results: After completing the exercise, you will have configured message-transport settings.

29 Proceed to Lab 7 - Exercise 2

30 Module 7 - Lab 7 - Exercise 2 - Configuring Email Protection

In this lab, you will continue in your role as Holly Dickson, Adatum's Enterprise Administrator. Adatum has experienced a recent rash of malware infections. The company's CTO has asked Holly to investigate the various options that are available in Exchange Online to fortify Adatum's messaging environment.

You will access the Exchange admin center for Exchange Online from your client computer and create a series of hygiene filters that are designed to protect Adatum's messaging environment. You will create a malware filter, a connection filter, and a spam filter. Finally, you will enable Microsoft 365 Advanced Threat Protection, which will safeguard Adatum against malicious threats posed by email messages, links (URLs), and collaboration tools.

30.0.1 Task 1 - Create a Malware Filter

In this task, you will create a malware filter that checks for attachments that have a specific file type that indicate a possible malware attachment. If an attachment is found matching one of those file types and the recipient's domain matches Adatum's Microsoft 365 domain, then default notification text will be applied to the message.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior lab, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **protection.**
4. At the top of the **protection** page, the **malware filter** tab is displayed by default. Stay in this tab.
5. On the menu bar, select the **plus (+) sign** icon to add a new malware filter.
6. In the **new anti-malware policy** window, enter **Malware Policy** in the **Name** field.
7. In the **Description** field, enter **This policy has been created to protect the messaging environment.**
8. Under **Malware Detection Response**, select **Yes and use the default notification text.**

9. Under **Common Attachment Types Filter**, select **On - Emails with attachments of filtered files types will trigger the Malware Detection Response (recommended).**
10. The filter will check for all the file types that appear in the **File Types** list. You do not need to add any additional file types, so proceed to the next step.
11. This filter will not generate any notifications, so scroll to the bottom of the page. Under **Applied To**, in the **If...** field, select the drop-down arrow and select **The recipient domain is.**
12. If a pop-up window displaying domains appears, then skip to the next step; otherwise, to the right of the condition field that displays **The recipient domain is...,** select **A recipient's domain is.**

    Note: The application usually displays the domain pop-up window at this point; however, if it doesn't, then you must select the **A recipient's domain is** to manually force it to display the domain window.
13. In the domain pop-up window that appears, select the **M365xZZZZZZ.onmicrosoft.com** domain (where ZZZZZZ is your tenant suffix ID provided by your lab hosting provider), select the **add ->** button, and then select **OK**.
14. Select **Save.**
15. Once the information has been successfully saved, select **OK** in the **information** window.
16. This returns you to the **malware filter** tab in the Exchange admin center. The new **Malware Policy** filter should be displayed in the list of filters. This filter should be selected, and a **Malware Policy** pane should appear on the right side of the screen that displays the conditions and actions of this filter. Verify the conditions and actions are correct; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
17. Leave the Exchange Admin Center open and proceed to the next task.

30.0.2 Task 2 - Create a Connection Filter

In this task, you will modify the default connection filter to include an allowed IP address and a blocked IP address. Any messages originating from the allowed IP address will always be accepted, and any messages originating from the blocked IP address will always be blocked.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior task, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior task, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, the **protection** tab in the left-hand navigation pane should still be selected from the prior task, and on this page, the **malware filter** tab should be displayed. Since you want to create a connection filter, select the **connection filter** tab at the top of the page.
4. In the list of connection filters, the **Default** filter is already selected by default. Select the **pencil (edit)** icon in the menu bar that appears above the filter list to edit this Default filter.
5. In the **Default** window, on the left-hand navigation pane, select **connection filtering.**

   Note: In this section you will be presented a variety of options on what IP Addresses will be allowed to send messages to your environment and what IP addresses will be blocked.
6. At this time, you will NOT be adding IP addresses to the allow or block lists. You can do this if you have a known IP address you would like to test against. However, it typically takes up to 1 hour to propagate the change within the system. For this lab, simply review the fact that you can create allowed and blocked lists of IP addresses.
7. Select the **Enable safe list** check box at the bottom of the page. This is a best practice that enables for your tenant the most common third-party sources of trusted senders that Microsoft subscribes to. Selecting this check box skips spam filtering on messages sent from these senders, ensuring that they are never mistakenly marked as spam.
8. Select **Save** and then select **OK** once the changes are successfully saved.
9. Leave the Exchange Admin Center open and proceed to the next task.

30.0.3 Task 3 - Create a Spam Filter

For Microsoft 365 customers whose mailboxes are hosted in Microsoft Exchange Online, their email messages are automatically protected against spam and malware. Microsoft 365 has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect you from spam.

As Adatum's Enterprise Administrator, Holly doesn't need to set up or maintain the filtering technologies, which are enabled by default. However, she can make company-specific filtering customizations in the Exchange admin center. She has decided to test this out by configuring a spam policy to grant or deny an email by focusing on the language of the email and the location of the email's origin.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior task, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior task, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, the **protection** tab in the left-hand navigation pane should still be selected from the prior task, and on this page, the **connection filter** tab should be displayed. Since you want to create a spam filter, select the **spam filter** tab at the top of the page.
4. In the list of spam filters, the **Default** filter is already selected by default. Select the **pencil (edit)** icon in the menu bar that appears above the filter list to edit this Default filter.
5. In the **Default** window, in the left-hand pane, select **spam and bulk actions**.

   Note: In this section you will be presented a variety of options on how you would like spam to be handled and what rating will be triggered depending on the severity of the spam.
6. In the **spam and bulk actions** section, make the following selections:
   - Spam: **Move message to Junk Email folder**
   - High Confident Spam: **Prepend subject line with text**
7. In the **Bulk email** section, make the following selections:
   - Mark bulk email as spam: Leave this check box selected
   - Select the threshold: select the drop-down arrow and change the threshold to **5**
8. In the **Quarantine** section, make the following selections:
   - Retain spam for (days): **10**
   - Prepend subject line with this text: enter **QUARANTINED: This message contains potential spam**
9. In the left-hand navigation pane, select **international spam**.

   Note: This section allows you to automatically tag messages as spam whose origins comes from countries/regions that are black listed, as well as messages written in a specific language.
10. Select the check box at the top of the page that says **Filter email messages written in the following languages**.
11. Select the **plus (+) sign** icon below this check box to add the languages being filtered.
12. In the **Select Language** window, hold down the **Ctrl** key and select the languages that you want to flag as spam. Then select the **add->** button, and then select **OK** to confirm your selection.
13. Below the list of languages that you selected, select the check box that says **Filter email messages sent from the following countries or regions**.
14. Select the **plus** (+) sign below this check box to add the countries or regions.
15. In the **Select Region** window, hold down the **Ctrl** key and select the countries or regions that you want to flag as being origins of spam. Then select the **add->** button, and then select **OK** to confirm your selection.

16. In the left-hand navigation pane, select **advanced options**.

    Note: This section allows you to automatically tag messages as spam that have embedded URL's with specific attributes or that have embedded HTML in the message.

17. Under the **Increase Spam Score** section, turn **On** the following options:

    - **URL redirect to other port**
    - **URL to .biz or .info websites**

18. Under the **Mark as Spam** section, turn **On** the following options:

    - **Empty messages**
    - **Conditional Sender ID filtering: hard fail**

19. Select **Save** and then select **OK** once the changes are successfully saved.

20. In the list of spam filters, the **Default** filter that you just edited is selected and a summary of the filter is now displayed in the right-hand pane. Scroll down in the right-hand pane and note how **End-user spam notifications** are disabled. Below this option, select **Configure end-user spam notifications**.

21. In the **edit end-user spam notifications** window, select the **Enable end-user spam notifications** check box, and then change the **Send end-user spam notifications every (days)** value to **5**.

22. Select **Save** and then select **OK** once the changes are successfully saved.

23. Leave the Exchange Admin Center open and proceed to the next exercise.

30.0.4 Task 4: Enable Advanced Threat Protection and Create a Safe Attachments Policy

In this task, you will turn on Advanced Threat Protection (ATP) for SharePoint, OneDrive, and Microsoft Teams, and you will create an ATP Safe Attachments policy that will test email attachments for malware that are sent to recipients within Adatum's M365xZZZZZZ.onmicrosoft.com domain. You will configure the policy so that if an attachment is blocked, it will be removed from the email that is sent to the recipient, and a copy of the email will be redirected to Joni Sherman for additional review.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**.

2. In your Edge browser session, open a new tab and enter the following URL in the address bar to open the **Office 365 Security and Compliance Center**: **https://protection.office.com.**

3. In the **Office 365 Security and Compliance center**, in the left-hand navigation pane select **Threat Management** and then select **Policy**.

4. In the **Policy** window, select the **ATP Safe Attachments** tile.

5. In the **Safe attachments** window, select **Global setting** on the menu bar.

6. In the **Global settings** window, at the top of the page under the **Protect files in SharePoint, OneDrive, and Microsoft Teams** section, select the **Turn on ATP for SharePoint, OneDrive and Microsoft Teams** toggle switch to **On** and then select **Save**.

7. On the **Safe attachments** page, select **+Create** on the menu bar to add a new Safe Attachments policy. This will initiate a **New Safe Attachment Policy** wizard to create a new policy.

8. On the **Name your policy** page, enter **AttachmentPolicy1** in the **Name** field and then select **Next**.

9. On the **Settings** page, under the **Safe attachments unknown malware response** section, select the **Dynamic Delivery** option. This option will still send the email but will hold the attachment until it has been scanned and marked acceptable.

10. Under the **Redirect attachment on detection** section, select the **Enable redirect** check box.

11. In the **Send the attachment to the following email address** field, enter Joni Sherman's email address of **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and then select **Next**.

12. On the **Applied To** page, select **+Add a condition**. In the drop-down menu that appears, under **Applied if**, select **The recipient domain is...**

13. This opens a box for defining the recipient domain. Select **Choose**.

14. In the **The recipient domain is** window, select **+Add**.
15. In the list of domains that appears, select the **M365xZZZZZZ.onmicrosoft.com** domain (where ZZZZZZ is your tenant ID provided by your lab hosting provider) and then select **Add**.
16. In the **The recipient domain is** window, the **M365xZZZZZZ.onmicrosoft.com** domain should in the **Domain name** list. Select **Done**.
17. On the **Applied to** page, select **Done**.
18. On the **Review your settings** page, review your entries and if anything needs to be changed, select the appropriate **Edit** link. If everything appears correct, select **Finish**.
19. Leave LON-CL1 and the Security and Compliance Center tab open for the next lab.

NOTE: Unfortunately, we are unable to create a training lab in which you can validate the ATP Safe Attachments policy that you just created. To do so, you must send an email that contains a malicious attachment. There are some common test viruses that are available, such as the EICAR test virus; however, with well-known test viruses such as EICAR, the messages in which they are attached get quarantined before they can be processed by Office 365 ATP. Since the ATP Safe Attachments functionality is meant to protect against unknown and zero-day viruses and malware, it is very difficult, and not recommended, to create such an attachment.

That being said, after you have defined ATP Safe Attachment policies in your real-world environment, one good way to see how the service is working is by viewing Advanced Threat Protection reports. For more information on using ATP reporting to validate your Safe Links and Safe Attachment policies, see View reports for Office 365 Advanced Threat Protection.

Results: After completing this exercise, you should have configured anti-spam and anti-virus settings.

31 Proceed to Lab 7 - Exercise 3

32 Module 7 - Lab 7 - Exercise 3 - Configuring client access policies

Outlook on the web enables Adatum's users to access their mailboxes through a web browser. After Adatum created its Microsoft 365 tenant with Exchange Online, the tenant included a single Outlook Web App policy titled OWAMailboxPolicy-Default. This policy defines Outlook on the web settings for all users. However, Holly Dickson, Adatum's Enterprise Admin, wants to create an additional Outlook on the web policy that applies to a specific user (in this case, Patti Fernandez). By verifying whether a user-specific policy such as this works, Holly will be able to vary the Outlook on the web settings for users with different needs.

Holly will then configure a mailbox policy for mobile devices that requires a password and sets the parameter for password length. Holly will then create a mobile device access policy that places any new devices into quarantine, at which point the device must be approved to be removed from quarantine so that it can send and receive messages.

32.1 Task 1: Configure an Outlook Web App policy

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior exercise, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **permissions**.
4. On the **permissions** page, the **admin roles** tab at the top of the page is displayed by default. Select the **Outlook Web App policies** tab.
5. On the the **Outlook Web App policies** tab, note the existing Outlook Web App policy titled **OWAMailboxPolicy-Default**. This policy defines Outlook on the web settings for all users.

   Since Holly wants to add a new policy, select the **plus (+) sign** icon on the menu bar.

6. In the **new Outlook Web App mailbox policy** window, enter **Limited features** in the **Policy name** field. Note - This policy is titled **Limited features** since it reduces the number of features that will be enabled for the policy.
7. The window displays a list of features that will be enabled for this Outlook Web App mailbox policy. The majority of these features are selected by default. Clear the check boxes for the following features that Holly does not want included in this custom policy:
   - **Instant messaging**
   - **Text messaging**
   - **Unified messaging**
   - **LinkedIn contact sync**
   - **Journaling**
8. At the bottom of the window, under **Private computer or OWA for devices**, clear the **Direct file access** check box, select **Save**, and then select **OK** once the information has been successfully saved.
9. In the **Exchange admin center**, in the left-hand navigation pane, select **recipients**.
10. On the **recipients** page, the **mailboxes** tab at the top of the page is displayed by default. In the list of user mailboxes, select **Patti Fernandez** and then select the **pencil (Edit)** icon on the menu bar.
11. In the **Patti Fernandez** window, in the left-hand navigation pane, select **mailbox features**.

    If you receive a **Warning** dialog box indicating the user hasn't logged on to the mailbox, so there is no data to return, select **OK**.
12. Scroll down to the **Email Connectivity** section and select **View details**.
13. In the **Outlook Web App mailbox policy** window, select **Browse**. This displays the list of existing Outlook Web App policies. Select **Limited features**, select **OK**, and then select **Save**.
14. In the **Patti Fernandez** window, select **Save** and then select **OK** once the information is successfully saved.
15. You will now open **Outlook 2016**. Select the Windows icon in the bottom left-hand corner of the taskbar. In the program menu that appears, scroll down and select **Outlook 2016**.

    If a **Microsoft Office Activation Wizard** appears that indicates this copy of Microsoft Office is not activated, select **Close**.
16. By default Outlook should open for the tenant admin account (the MOD Administrator, whose email address is admin@M365xZZZZZZ.onmicrosoft.com). However, if you are instead prompted for user credentials in a **Windows Security** dialog box, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and enter the tenant admin password provided by your lab hosting provider.
17. In **Outlook 2016**, select **New Email**.
18. In the **new email** window, select the **To** button, and in the list of users that appears, select **Patti Fernandez**, select **To**, and then select **OK**.
19. In the **Subject** box, enter **Attachment Test**.
20. In the ribbon, select **Attach File**, and then Select **Browse This PC**.
21. In the **Insert File** window, browse to **C:\Windows\Logs\DISM**, select **dism.log**, and then select **Insert**.
22. Select **Send**.
23. After sending the email, close Outlook 2016.
24. Switch to **LON-CL2**.
25. **Outlook on the web** should still be open from a previous lab; however, you should be logged in as the MOD Administrator from the first exercise in this lab. Therefore, you must log out from Outlook as the MOD Administrator and log back in as Patti.

To do so, select the MOD Administrator's user icon (the circle with the **MA** initials) in the upper right corner of the screen, then select **Sign out** in the **My account** window, enter **https://outlook.office365.com** in the address bar, sign in as Patti Fernandez (**PattiF@M365xZZZZZZ.onmicrosoft.com**, where ZZZZZZ is the tenant ID provided by your lab hosting provider), and enter the password assigned to the tenant admin account by your lab hosting provider.

26. In Patti's **Inbox**, select the email that you just sent from the **MOD Administrator** that contains the **Attachment Test** subject.
27. Select the **dism.log** message attachment.
28. A message should appear indicating that you do not have permission to download files.

    Note: In some cases, it may take a few minutes for the new Outlook Web App mailbox policy to take effect, so you may not see this message at this time.
29. Close the message attachment window.
30. Leave Outlook on the web open for Patti Fernandez.
31. Leave the Edge browser open and and all its tabs.

32.2 Task 2: Configure mobile-device access

In this task, you will create a mobile device access policy that places any new devices into quarantine, at which point the device must be approved to be removed from quarantine so that it can send and receive messages.

1. Switch to **LON-CL1**, where you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior exercise, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **mobile**.
4. On the **mobile** page, the **mobile device access** tab at the top of the page is displayed by default.
5. On the **mobile device access** tab, under the **Exchange ActiveSync Access Settings** section, select the **edit** button that appears at the far right of the screen.
6. In the **Exchange ActiveSync access settings** window, under the **Connect Settings** section, select the **Quarantine – Let me decide to block or allow later** option.
7. Under the **Quarantine Notification Email Messages** section, select the **plus (+) sign (Add) ** icon to add an administrator to receive email messages when a mobile device is quarantined.
8. In teh **Select Administrators** window, in the list of users, select **MOD Administrator**, select **add**, and then Select **OK**.
9. In the **Exchange ActiveSync access settings** window, select **Save**.
10. Leave the Edge browser open and and all its tabs.

32.3 Task 3: Configure a mailbox policy for mobile devices

In this task, you will configure a mailbox policy for mobile devices that requires a password and sets the parameter for password length.

1. You should still be logged into **LON-CL1** as the **Administrator** with a password of **Pa55w.rd**.
2. Your Edge browser should be open from the prior exercise, with tabs open for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **Exchange admin center**. You should still be signed into Microsoft 365 as Holly Dickson.

   If you closed the Exchange admin center tab after the prior lab exercise, then in the **Microsoft 365 Admin center**, under **Admin Centers** in the left-hand navigation pane, select **Exchange**.

3. In the **Exchange admin center**, you should still be displaying the **mobile** tab in the left-hand navigation pane..
4. On the **mobile** page, the **mobile device access** tab at the top of the page should still be displayed from the prior task. Select the **mobile device mailbox policies** tab.
5. On the **mobile device mailbox policies** tab, select the **Default (default)** policy and then select the **pencil (Edit)** icon on the menu bar.
6. In the **Default** window, select the **security** tab in the left-hand navigation pane.
7. In the **security** tab, select the **Require a password** check box that appears at the top of the window.
8. Select the **Allow simple passwords** check box (if it's not already selected).
9. Select the **Minimum password length** check box, enter a value of **6**.
10. In the **Password recycle count** check box, enter a value of **5**, select **Save**, and then select **OK** once the information is successfully saved.
11. Leave the Edge browser and all its tabs open.

33 End of Lab 7

33.1 Module 8 - Lab 8 - Exercise 1 - Configure Microsoft Teams

In this exercise you will learn how to manage and configure Microsoft Teams through the Teams admin center. As Holly Dickson, Adatum's Enterprise Admin, you have decided to customize the company's Global meeting policy. Meeting policies control the features that are available to participants in meetings that are scheduled by users in an organization. An organization-wide policy named Global is created by default, and all users within the organization are automatically assigned this meeting policy. An admin can either make changes to this policy or create one or more custom policies and assign users to them. Holly has chosen to customize the Global policy.

Holly also wants to use the Teams meetings settings to control whether anonymous users can join Teams meetings and customize meeting invitations. As part of Adatum's pilot project for implementing Microsoft Teams, she has been tasked with configuring Teams meeting settings to see how they handle email invitations.

Next, Holly wants to create a new messaging policy that addresses the chat and channel messaging requirements set forth by Adatum's project team. She will then create a resource account for a cloud call queue, which is a service that accepts customer calls, plays a greeting message, and then places the customer calls in a wait queue while searching a pre-configured list of agents to answer each call. Once she has created the resource account for her calling queue, she will create the call queue itself and assign it the resource account.

At this point, Holly will turn her attention to calling policies. She has been tasked with creating a custom calling policy for Adatum. Instead of customizing the default global policy, she will follow best practice guidelines and create her own customized policy that will be used as Adatum's default policy.

Finally, Holly wants to manage Teams access, and specifically external access and guess access. She wants to block communication with users from a specific domain that has been the source of multiple spam attacks within Adatum over the past year. At the same time, she wants to allow communication with the users from another domain that is one of Adatum's key business partners.

33.1.1 Task 1 – Manage Global Meeting Policy

Meeting policies control the features that are available to participants in meetings that are scheduled by users in your organization. An organization-wide policy named Global is created by default, and all users in your organization are automatically assigned this meeting policy. You can either make changes to this policy or create one or more custom policies and assign users to them. When you create a custom policy, you can allow or prevent certain features from being available to your users, and then assign the policy to one or more users who will have the settings applied to them.

As Holly Dickson, Adatum's Enterprise Administrator, you want to customize the company's Global meeting policy as part of Adatum's pilot project for implementing Microsoft Teams.

1. Switch to **LON-DC1**, where you should still be logged in as **ADATUM\Administrator** and password **Pa55w.rd**.

2. You should still have Microsoft Edge and the Microsoft 365 admin center open from an earlier lab. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) with a password of **Pa55w.rd**, and then in the **Microsoft Office Home** page, select **Admin** to open the Microsoft 365 admin center.
3. To start fresh in this Teams lab exercise, close any tab in the Edge browser other than the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab.
4. In the **Microsoft 365 admin center** tab, in the left-hand navigation pane, select **Show all** (if necessary), then scroll down to **Admin centers** and select **Teams.** This will open the **Microsoft Teams admin center** in a new tab.
5. If a **Welcome to the Teams admin center** window appears, select the **Skip tour** option.
6. In the **Microsoft Teams admin center**, in the left-hand navigation pane, select **Meetings** and then select **Meeting policies**.
7. In the **Meeting policies** window, scroll down to the list of meeting policies and select **Global (Org-wide default)**.
8. In the **Global** window that appears, under the **General** section, review each setting. All settings in this section should be turned **On**.
9. Under the **Audio & video** section, review each setting. Set **Allow transcription** to **On**.
10. Under the **Content Sharing** section, review each setting. Select the drop-down arrow in the **Screen sharing mode** field and select **Single application** and then set the **Allow an external participant to give or request control** setting to **On**.
11. Under the **Participants & guests** section, review each setting. Because Adatum has had issues in the past with non-invited external users dialing into meetings, you have been asked to set the **Allow dial-in users to bypass the lobby** option to **Off**. This setting controls whether people who dial in by phone will automatically join the meeting or must wait in the lobby until they are admitted to the call. Because the **Automatically admit people** setting is set to **Everyone in your organization**, anyone who dials-in will wait in the lobby until admitted; this includes both Adatum and non-Adatum participants. You may decide to turn this setting **On** if it proves to be problematic in practice, but for now, you want to begin with this level of control.
12. Select the **Save** button at the bottom of the page.
13. Leave all tabs open in your browser and proceed to the next task.

33.1.2 Task 2 – Manage Meeting Settings

As Holly Dickson, Adatum's Microsoft 365 Enterprise Administrator, you use the Teams meetings settings to control whether anonymous users can join Teams meetings and customize meeting invitations. You can also use these settings to enable Quality of Service (QoS) and set port ranges for real-time traffic. These settings apply to all Teams meetings that users schedule in your organization. As part of Adatum's pilot project for implementing Microsoft Teams, you want to configure Teams meeting settings to see how they handle email invitations.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, under the **Meetings** group, select **Meeting settings.**
2. On the **Meetings settings** page, under the **Email invitation** section, enter (or copy and paste in) the following information:
   - Logo URL: leave blank
   - Legal URL: **https://adatum.com/legal.html**
   - Help URL: **https://adatum.com/joiningmeetinghelp.html**
   - Footer: **Please accept at your earliest convenience. Thank you!**
3. Select the **Preview invite** button.
4. On the **Email invite preview** window, review the preview image of the invitation and then select the **Close** button at the bottom of the page.

5. On the **Meetings settings** page, under the **Network** section, review the current settings.

   Note: If you have specific ports that your company uses for sending and receiving media traffic, this is where you would enter those ports. If you do not have specific media ports prescribed by your network administrator, then you would leave this section alone. For the purposes of this lab, you will not update this section.

6. Scroll to the bottom of the page and select **Save**.
7. Leave all tabs open in your browser and proceed to the next task.

33.1.3 Task 3 – Manage Messaging Policies

Messaging policies are used to control which chat and channel messaging features are available to users in Microsoft Teams. You can use the Global default policy that is created automatically or create one or more custom messaging policies for people in your organization. After you create a policy, you can assign it to a user or group of users in your organization.

As part of her Microsoft Teams pilot project for Adatum, Holly wants to create a new messaging policy that addresses the chat and channel messaging requirements set forth by Adatum's project team.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, select **Messaging policies**.
2. In the **Messaging policies** window, view the list of messaging policies. As you can see, only the **Global (Org-wide default)** policy exists. Select **+Add** in the menu bar that appears above the list of policies.
3. In the **Messaging policies\Add** window, enter **Chat and Channel Messaging Policy** in the **New messaging policy** field at the top of the form.
4. Select the following values for each setting:
   - Owners can delete sent messages: **Off**
   - Delete sent messages: **Off**
   - Edit sent messages: **On**
   - Read receipts: **Turned on for everyone**
   - Chat: **On**
   - Use Giphy in conversations: **Off**
   - Giphy content rating: **Strict**
   - Use Memes in conversations: **Off**
   - User Stickers in conversations: **Off**
   - Allow URL previews: **On**
   - Translate messages: **On**
   - Allow immersive reader for viewing messages: **On**
   - Send urgent messages using priority notifications: **On**
   - Create voice messages: **Allowed in chats and channels**
   - On mobile devices, display favorite channels about recent chats: **Disabled**
   - Remove users from a group chat: **Off**
   - Suggested replies: **On**
5. Select **Save.**
6. Leave all tabs open in your browser and proceed to the next task.

33.1.4 Task 4 – Create a Resource Account

A resource account, which is referred to as a disabled user object in Azure Active Directory, can be used to represent resources in general. For example, a resource account in Exchange can be used to represent conference rooms, and in Microsoft Teams, resource accounts can be used to represent Phone System call queues and auto attendants.

As part of Adatum's pilot project for implementing Microsoft Teams, Holly Dickson has been asked to create a resource account for a cloud call queue, which is a service that accepts customer calls, plays a greeting message, and then places the customer calls in a wait queue while searching a pre-configured list of agents to answer each call.

Creating a calling queue is a two-step process. In this task, you will first create a resource account that represents the call queue. In the next task, you will create the actual call queue and associate it with this resource account.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, select **Org-wide Settings** and then select **Resource accounts.**
2. In the **Resource accounts** window, select **+Add** in the menu bar at the top of the page.
3. In the **Add resource account** pane that appears on the right, enter the following information:
   - Display name: **Calling Queue 1**
   - Username: **CQ1**
   - Domain name: In the domain name field to the right of the username, select the drop-down arrow and select **M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
   - Resource account type: **Call queue**
4. Select **Save**. **Calling Queue 1** will now appear in the list of Resource accounts.
5. Leave all tabs open in your browser and proceed to the next task.

33.1.5 Task 5 - Create a Call Queue

Now that you have created the resource account for your calling queue, you will create the call queue itself and assign it the resource account.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, select **Voice** and then select **Call queues.**
2. In the **Call queues** window, select **+Add** in the menu bar at the top of the page.
3. In the **Call queues\Add** window, enter **Call Queue 1** in the **Call queue name** field at the top of the form.
4. The page displays a message indicating **You haven't added any resource accounts yet.** Below this message, select the **Add accounts** button.
5. In the **Add account** pane that appears on the right-side of the screen, in the **Search for resource accounts you want to add** box, enter **Calling.** As you type **Calling**, a window appears listing call resource accounts whose title starts with **Calling**. **Calling Queue 1** is displayed. As you hover your mouse over **Calling Queue 1**, an **Add** button appears to the right of it. Select the **Add** button.
6. At the bottom of the **Add accounts** pane, select **Add.** This returns you to the **Call Queue 1** window, which now displays **Calling Queue 1** in the list of Resource accounts associated with this call queue.
7. In the **Call Queue 1** window, scroll down the page and select the following values for each option:
   - Greeting: **No greeting**
   - Music on hold: **Play default music**
   - Call answering:
     - **Choose which call agents to associate with this call queue:** Select the **Add users** button. In the **Add users** pane that appears on the right-side of the screen, in the **Add a user or users** box, enter **Allan**. As you type **Allan**, a window appears listing users whose name starts with

Allan. As you hover your mouse over **Allan Deyoung**, an **Add** button appears to the right of it. Select the **Add** button.

Important: Note the red error message that appears across the top of the page. The error message indicates that Allan cannot be associated with this call queue because he is not enterprise-voice enabled. In the **Add users** window, select **Cancel**. In the red error message, select the **X** on the right side of the error message to close it.

- **Choose which groups to associate with this call queue:** Select the **Add groups** button. In the **Add call agents** pane on the right-side of the screen, in the **Add distribution lists or groups** box, enter **Sales.** As you type Sales, a window appears listing the groups whose name starts with Sales. As you hover your mouse over **Sales Department**, an **Add** button appears to the right of it. Select the **Add** button.

In the **Add call agents** pane, the Sales Department appears under **Selected groups**. Select the **Add** button at the bottom of the pane.

- Routing Method: **Round Robin**
- Presence-based routing - **Off**
- Agents can opt out of taking calls: **On**
- Agent alert time (in seconds) - 45 (entering the value in the field is easier than dragging the slider icon)

- Call overflow handling: **leave all settings to their default values**
- Call time out handling: **leave all settings to their default values**

8. Select **Save**. A Saved message will appear across the top of the page once the changes have been saved. This message will eventually disappear, and **Call Queue 1** will appear in the list of Call queues.
9. Leave all tabs open in your browser and proceed to the next task.

33.1.6 Task 6 - Create a Calling Policy

In Microsoft Teams, calling policies control which calling and call forwarding features are available to users. Calling policies determine whether a user can make private calls, use call forwarding or simultaneous ringing to other users or external phone numbers, route calls to voicemail, send calls to Call Groups, use delegation for inbound and outbound calls, and so on. A default global policy is created automatically, but admins can also create and assign custom calling policies.

As part of her Microsoft Teams pilot project, Holly Dickson has been tasked with creating a custom calling policy for Adatum. Instead of customizing the default global policy, she will follow best practice guidelines and create her own customized policy that will be used as Adatum's default policy.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, under the **Voice** group, select **Calling policies.**
2. In the **Calling policies** window, scroll down through the list to see the predefined calling policies and then select **+Add** in the menu bar that appears above the list of calling policies.
3. In the **Calling policies\Add** window, enter **Default Adatum Calling Policy** in the **Add new calling policy** field at the top of the form.
4. Scroll down the page and select the following values for each setting:
   - Make private calls: **On**
   - Call forwarding and simultaneous ringing to people in your organization: **Off**
   - Call forwarding and simultaneous ringing to external phone numbers: **On**
   - Voicemail is available for routing inbound calls: **Enabled**
   - Inbound calls can be routed to a call group: **On**
   - Allow delegation for inbound and outbound calls: **Off**
   - Prevent toll bypass and send calls through the PSTN: **On**
   - Busy on busy is available when in a call: **On**

- Allow web PSTN calling: **On**

5. Select **Save**. A Saved message will appear across the top of the page once the changes have been saved. This message will eventually disappear, and **Default Adatum Calling Policy** will appear in the list of Calling policies. Note how it is flagged as a Custom policy.
6. Leave all tabs open in your browser and proceed to the next task.

33.1.7 Task 7 – Manage External Access

With Microsoft Teams' external access feature, Teams users from other domains can participate in your chats and calls. You can also block the users in specific domains from joining chats and calls.

As part of her Microsoft Teams pilot project, Holly Dickson wants to block communication with users from a specific domain (spam.com) that has been the source of multiple spam attacks within Adatum over the past year. At the same time, Holly wants to allow communication with the users from another domain (microsoft.com) that is one of Adatum's key business partners.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, under the **Org-wide settings** group, select **External access.**
2. In the **External access** window, leave the first two settings involving Skype for Business/Teams and Skype users set to **On**.
3. To add the domain in which you want to allow communication, select **+Add a domain** in the menu bar that appears above the list of domains.
4. In the **Add a domain** window, enter the following information:
   - Domain: **microsoft.com**
   - Action to take on this domain: **Allowed**
5. Select **Done.**
6. To add the blocked domain, in the **External access** window, select **Add a domain.**
7. In the **Add a domain** pane that appears on the right, enter the following information:
   - Domain: **spam.com**
   - Action to take on this domain: **Blocked**
8. Select **Done.**
9. In the **External access** window, validate that **microsoft.com** and **spam.com** are represented in the list of domains and that each has the appropriate Status.
10. Select **Save.**
11. Leave all tabs open in your browser and proceed to the next task.

33.1.8 Task 8 – Manage Guest Access

Microsoft Teams' guest access feature is a tenant-level setting that is turned Off by default. Once this setting is turned On, you can configure settings for guests. IT admins can add guests at the tenant level, set and manage guest user policies and permissions, and generate reports on guest user activity.

As part of your Microsoft Teams pilot project for Adatum, you will turn on guest access and then customize a variety of the guest settings as defined by Adatum's project team.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, under the **Org-wide settings** group, select **Guest access.**
2. In the **Guest access** window, set the **Allow guest access in Teams** setting to **On**.
3. Once you set this switch to **On**, a variety of additional settings are displayed. Scroll down the page and select the following values for each setting:
   - Calling
     - Make private calls: **Off**
   - Meeting

- Allow IP video: **On**
- Screen sharing mode: **Entire screen**
- Allow Meet Now: **On**

- Messaging
  - Edit sent messages: **Off**
  - Delete sent Messages: **Off**
  - Chat: **On**
  - Use Giphy in conversations: **Off**
  - Giphy content rating: **Strict**
  - Use Memes in conversations: **Off**
  - User Stickers in conversations: **Off**
  - Allow immersive reader for viewing messages: **On**

4. Select **Save.** Note the message that displays indicating it can take a couple of hours for the changes to take effect. This message does not automatically disappear, so close this message by selecting the **X** that appears at the right-side of the message; otherwise, the message will remain at the top of your screen even as you navigate to other pages.
5. Leave all tabs open in your browser and proceed to the next task.

33.1.9 Task 9 – Manage Teams Settings

Microsoft Teams includes a variety of global settings that control performance within Teams. As part of her Microsoft Teams pilot project, Holly Dickson will configure a number of these settings as determined by Adatum's project team.

1. On **LON-DC1** you should still have the **Microsoft Teams admin center** open from the prior task. In the left-hand navigation pane, under the **Org-wide settings** group, select **Teams settings.**
2. In the **Teams settings** window, select the following values for each setting:
   - Notifications and feeds
     - Suggested feeds can appear in a user's activity feed: **On**
   - Tagging
     - Tags are managed by: **Team owners and members**
     - Let team owners override who can manage tags: **On**
     - Suggested tags: **Sales** (press the space bar after entering this value); **Manufacturing** (press the space bar after entering this value); **Accounting** (press the space bar after entering this value)
     - Let custom tags be created: **On**
   - Email integration
     - Allow users to send emails to a channel email address: **On**
     - Accept channel email from these SMTP Domains: **microsoft.com** (press the space bar after entering this value)
   - Files
     - Citrix files: **On**
     - DropBox: **Off**
     - Box: **Off**
     - Google Drive: **On**
     - Egnyte: **Off**
   - Organization

- Show Organization tab in chats: **On**

- Devices
  - Require a secondary form of authentication to access meeting content: **No access**
  - Set content PIN: **Required for outside scheduled meeting**
  - Resource accounts can send messages: **On**

- Search by name
  - Scope directory search using an Exchange address book policy: **On**

3. Select **Save.** Note the message that appears at the top of the form that it may take a few hours to see these changes applied.
4. Leave all tabs open in your browser and proceed to the next task.

34 End of Lab 8

35 Module 9 - Lab 9 - Exercise 1 - Configuring SharePoint Online settings

Now that Holly Dickson has configure Exchange Online and Microsoft Teams, she will begin preparing Adatum to implement SharePoint Online within the organization's Microsoft 365 pilot project. In this exercise, Holly will begin by configuring SharePoint Online settings to meet Adatum's business needs.

35.0.1 Task 1 - Configure settings

1. Switch to **LON-CL1**, where you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. You should still have Microsoft Edge and the Microsoft 365 admin center open from an earlier lab. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and a passworf of **Pa55w.rd**, and then in the **Microsoft Office Home** page, select **Admin** to open the Microsoft 365 admin center.
3. To start fresh in this SharePoint lab exercise, close any tab in the Edge browser other than the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab.
4. In the **Microsoft 365 admin center** tab, in the left-hand navigation pane, select **Show all** (if necessary), then scroll down to **Admin centers** and select **SharePoint**. This will open the **SharePoint admin center** in a new tab.
5. On the left-hand navigation pane, select **Settings**.
6. On the **Settings** page, below the list of settings is a message indicating that if you can't find the setting you're looking for to go to the **classic settings page**. Select **classic settings page**. This will open a new tab with the **Settings** page from the classic SharePoint admin center.
7. On the classic **Settings** page, scroll down to the **Enterprise Social Collaboration** group. To the right of this group are two options. Select **Use Yammer.com service**.
8. Scroll to the bottom of the page and select **OK**.
9. Close this tab for the classic **Settings** page. You should now be back on the **Sharepoint admin center** tab in the Edge browser.
10. In the left-hand navigation pane, select **Policies** and then select **Sharing**.
11. On the **Sharing** page, select **More external sharing settings** to expand this group of settings. Within this group of external sharing settings, select the **Guests must sign in using the same account to which sharing invitations are sent** check box, and select the **Allow guests to share items they don't own** check box (if it's not already selected by default). Scroll to the bottom of the window and select **Save**.
12. Leave all tabs open in your browser and proceed to the next task.

35.0.2 Task 2 - Configure user profiles

1. On **LON-CL1** you should still have the **SharePoint admin center** open from the prior task. In the left-hand navigation pane, select **More features**.
2. On the **More features** page, in the **User profiles** group, select **Open**.
3. On the **User Profiles** page, under the **People** group, select **Manage User Profiles**.
4. On the **User Profiles** page, enter **PattiF** in the **Find profiles** field and then select **Find**. Patti Fernandez's account will appear in the account name list.
5. In the list of accounts, select the **Account name** for **Patti Fernandez**. In the drop-down menu that appears, select **Edit My Profile**.
6. In the **User Profiles** page, in the **Manager** field, enter **Admin**. Then select the **check names** icon to the right of the field and verify the field displays **MOD Administrator**.
7. In the upper-right corner of the page, select **Save and Close**.
8. Close the **Manage User Profiles** tab in your browser. This should return you back to the **SharePoint admin center** tab.
9. On the **SharePoint admin center** tab, it should still be displaying the **More features** page. In the **User profiles** group, select **Open**.
10. On the **User Profiles** page, under the **My Site settings** group, select **Setup My Sites**.
11. In the **My Site Settings** tab, scroll down to the **My Site Cleanup** section.
12. In the **Secondary Owner** field, enter **Admin** and then select the **Check names** icon. Verify the field displays **MOD Administrator**.
13. Scroll down to the bottom of the page and select **OK**.
14. Close the **Manage Profile Service** tab in your Edge browser.
15. Leave all tabs open in your browser and proceed to the next task.

35.0.3 Task 3 - Configure apps

1. On **LON-CL1** you should still have the **SharePoint admin center** open from the prior task, and it should be displaying the **More features** page.
2. On the **More features** page, under the **Apps** group, select **Open**.
3. On the **Apps** page, select **Configure Store Settings**.
4. In the **Apps for Office from the Store** setting, select **No** to disable apps from starting when documents are opened in the browser.
5. Select **OK**.
6. Close the **Apps** tab in your browser.

Results: After completing this exercise, you should have configured SharePoint Online service settings.

36 Proceed to Lab 9 - Exercise 2

37 Module 9 - Lab 9 - Exercise 2 - Configuring SharePoint Online site collections

In this exercise, Holly Dickson wants to begin exploring SharePoint Online site collections. A site collection is made up of one top-level site and all sites below it. For comparison purposes, Holly plans to create a site collection using the SharePoint Online admin center, followed by a second site collection using Windows PowerShell. She will then configure access permissions to the site collections, and then follow that up by verifying the access permissions work.

37.1 Task 1: Create a site collection using the SharePoint admin center

In this task, you will use the SharePoint admin center to create a site collection for Adatum's Marketing department.

1. On **LON-CL1** you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. You should still have Microsoft Edge open from the previous exercise, along with tabs for the **Microsoft Office Home** page, the **Microsoft 365 admin center**, and the **SharePoint admin center**. If so, select the **SharePoint admin center** and proceed to the next step.

   Otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and a password of **Pa55w.rd**, and then in the **Microsoft Office Home** page, select **Admin** to open the Microsoft 365 admin center, select **Show all** in the left-hand navigation pane, and then under **Admin centers** select **Sharepoint**.
3. In the **SharePoint admin center**, in the left-hand navigation pane, select **More features**.
4. On the **More features** page, scroll to the bottom and in the **Classic site collections page** section, select **Open**.
5. On the **Site collections** page, in the ribbon, select **New**, and then in the drop-down menu that appears, select **Private Site Collection**.
6. In the **new site collection** window, enter **Marketing** in the **Title** field.
7. In the **Web Site Address** field, in the blank field to the right of **/sites/**, enter **Marketing**.
8. In the **Administrator** field towards the bottom of the window, enter **Admin** and then select the **Check Names** icon. Once the value is verified, it will be replaced with **MOD Administrator**.
9. Leave the default values unchanged for the other settings and then select **OK**. This will return you to the **Site collections** page.

Note: It can sometimes take a few minutes for SharePoint Online to provision a new site. Eventually, the **Marketing** site will appear in the list of site collections. Do not proceed to the next step until the **Marketing** site appears in the list.

10. On the **Site collections** page, hover your mouse over the **URL** for the marketing site. Select the check box that appears to the left of the of the **Marketing** site's URL.
11. Selecting the check box for the marketing site will trigger the **Sharing** menu to appear on the ribbon. However, it may take a few minutes for the **Sharing** menu to appear. You can speed this up by refreshing the page by selecting the **Refresh** icon to the left of the address bar, or by pressing the F5 key.
12. Select **Sharing** once the Sharing menu appears on the ribbon.
13. In the **sharing** window, select **Allow sharing with all external users, and by using anonymous access links** and then select **Save**.

Note: The site settings changes to allow external user sharing. This process is usually done within one minute. External user sharing is now enabled and you can use it for this marketing site.

14. Leave your Edge browser and all its tabs open and proceed to the next task.

37.2 Task 2: Create a site collection using Windows PowerShell

Now that you have experience creating a site collection using the SharePoint admin center, you will use Windows PowerShell to create a site collection for Adatum's Accounting department. This will provide you with experience using both mechanisms to create site collections.

1. You should still be logged into **LON-CL1** and you should have the **SharePoint admin center** open from the prior task.
2. In this task, you will use **Windows PowerShell** to create a SharePoint site collection. To do so, you must first install the **SharePoint Online Management Shell** from the **Microsoft Download Center**.

   Open a new tab in your **Microsoft Edge browser** and enter the following URL in the address bar: **http://aka.ms/f04q5o**.

3. In the **Microsoft Download Center**, scroll down to the **SharePoint Online Management Shell** section and select the **Download** button.
4. On the **Choose the download you want** page, select the check box for the **64-bit** (x64) version and then select **Next**.
5. If a message about pop-ups appears, select **Allow once**.
6. Once the download is complete, the file will appear in the notification bar at the bottom of your screen. Select **Open file**.
7. After a short delay, the **SharePoint Online Management Shell Setup** wizard will open. On the **License Agreement** page, select the **I accept the terms in the License Agreement** check box and then select **Install**.
8. If a **User Account Control** dialog box appears asking if you want to allow this app to make changes to your device, select **Yes**.
9. When the installation completes, Select **Finish**.
10. Select the **Windows** icon on the bottom left corner of the taskbar. In the **Start** menu that appears, in the **Recently added** group at the top of the menu, right-click on **SharePoint Online Management Shell**. In the menu that appears, select **More** and then in the next menu, select **Run as administrator**.
11. In the **User Account Control** dialog box, select **Yes** to allow this app to make changes to your device.
12. Maximize the **SharePoint Online Management Shell** window. At the command prompt, type the following command and then press Enter (where ZZZZZZ is the unique tenant ID provided by your lab hosting provider):

    ```
    Connect-SPOService -Url https://M365xZZZZZZ-admin.sharepoint.com -credential admin@M365xZZZZZZ.onm
    ```

13. In the **Enter your credentials** dialog box, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then Select **OK**.
14. At the command prompt, type the following command and then press Enter to add a new site collection titled **Accounting** (where ZZZZZZ is the tenant ID provided by your lab hosting provider):

    ```
    New-SPOSite -Url https://M365xZZZZZZ.sharepoint.com/sites/Accounting -Owner Admin@M365xZZZZZZ.onmi
    Title "Accounting"
    ```

15. Close the **SharePoint Online Management Shell** window.
16. In your Edge browser, the **Site collections** page should still be displayed from the prior task. If the new **Accounting** site collection does not appear in the list of site collections, select the **Refresh** icon that appears to the left of the address bar. Do not proceed to the next step until you have verified that the new **Accounting** site collection appears in the Site Collections list.
17. In your Edge browser, close the **Manage site collections** tab and the **Download SharePoint Online Management Shell** tab.
18. Leave your Edge browser open along with the **Microsoft Office Home** tab, the **Microsoft 365 admin center** tab, and the **SharePoint admin center** tab, and then proceed to the next task.

37.3 Task 3: Configure permissions on the site collections

Now that you have added site collections for Adatum's Marketing and Accounting departments, you will configure permissions for the Marketing site collection. Because you are still signed into Microsoft 365 as Holly Dickson, you must open an In-Private browser session in Edge and log into Microsoft 365 as the MOD Administrator so that you can assign Patti Fernandez as an admin to the Marketing site.

Only a site's site admin can assign another user as an admin to the site. While you are signed into Edge as Holly Dickson, she is not an admin for the Marketing site. Therefore, you will have to open an InPrivate session so that you can log in as the MOD Administrator to make this assignment.

You will then open a second InPrivate browsing session and log in as Patti Fernandez to verify that she is a site admin for the Marketing site. You will do this by accessing the Marketing site's **Site Collection Administrators** page, which is only accessible to site admins.

1. On **LON-CL1**, right-click on the **Edge** icon on the taskbar, and in the menu that appears, select **New InPrivate window**.

2. In your **InPrivate Browsing** session, enter the following URL in the address bar: **https://portal.office.com**.
3. In the **Sign in** window, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
4. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
5. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
6. On the **Microsoft Office Home** page, select **Admin**.
7. On the **Microsoft 365 admin center** page, in the left-hand navigation pane, select **Show all**, and then under the **Admin centers** group, select **SharePoint**.
8. On the **SharePoint admin center** page, in the left-hand navigation pane, select **Sites**, and then select **Active Sites**.
9. On the **Active sites** page, note the **Marketing** and **Accounting** site collections appear in the list of active sites. Select the **Marketing** site.
10. At the time you created the **Marketing** site, the MOD Administrator was added as a site admin. You now want to add **Patti Fernandez** as a second site administrator.

    On the **Marketing** pane that appears on the right-side of the screen, select the **Permissions** tab.
11. In the **Permissions** tab, under the **Site admins** section, select **Manage**.
12. On the **Manage admins** page, in the **Add an admin** field, enter **Patti**. This will display a list of all active users whose first name starts with Patti. In the list of users that appears, select **Patti Fernandez** and then select **Save**. Patti and the MOD Administrator should now appear as admins for this site.
13. Close the **Marketing** pane.
14. Close the **InPrivate** browsing session for the **MOD Administrator**.
15. Perform the same steps as before to open a new **InPrivate** browsing session, this time for **Patti Fernandez**.
16. In your new **InPrivate** browsing session, enter the following URL in the address bar: **https://portal.office.com**
17. On the **Pick and account** dialog box, select **Use another account**.
18. In the **Sign in** window, enter **PattiF@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
19. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
20. This opens the **Microsoft Office Home** tab in your InPrivate browsing session. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketin** (where ZZZZZZ is the tenant ID provided by your lab hosting provider).
21. This opens the **Marketing** site collection. In the upper-right corner of the screen (to the left of Patti's picture), select the **gear (Settings)** icon (the wheel icon). In the **Settings** window that appears, select **Site settings**.
22. On the **Site Settings** page, under the **Users and Permissions** group, select **Site collection administrators**.
23. Verify that **MOD Administrator** and **Patti Fernandez** appear in field. You have just verified that Patti is indeed a site administrator for the Marketing site collection, since she can access the Site Collection Administrators page (only site admins can access this page).
24. Close the **InPrivate** browsing session for **Patti Fernandez**.
25. Leave your Edge browsing session open along with all its tabs.

37.4 Task 4: Verify access to the site collections

In this task, the MOD Administrator will assign access to the Marketing site collection to two users - Joni Sherman, who requested access in the prior task, and Nestor Wilke, who the MOD Administrator felt should have access as well since Nestor is a company Director. While Nestor did not request access, the MOD Admin

will share access to the site with him. You will again use InPrivate browsing sessions for the different users to access the Marketing site on LON-CL1.

1. On **LON-CL1**, right-click on the **Edge** icon on the taskbar, and in the menu that appears, select **New InPrivate window**.
2. In your **InPrivate Browsing** session, enter the following URL in the address bar: **https://portal.office.com**.
3. In the **Sign in** window, enter **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
4. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
5. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
6. This opens the **Microsoft Office Home** tab in your Edge browser. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketing** (where ZZZZZZ is the tenant ID provided by your lab hosting provider).
7. This displays an **Access required** page that indicates **You need permission to access this site.** A message field is prefilled with the following default message: **I'd like access, please**.

   Since you can customize this message, Joni wants to enter a message that justifies why he needs permission to access this site. Replace the existing message with the following: **My name is Joni Sherman. I am a Technical Account Manager for Western Europe. I need access to this site so that I can stay abreast of the latest marketing plans for Adatum's Fabrication division.**
8. Select the **Request Access** button.
9. Close this InPrivate browsing session for **Joni Sherman**.
10. Perform the same steps as before to open a new **InPrivate** browsing session, this time for the **MOD Administrator**.
11. In your new **InPrivate** browsing session, enter the following URL in the address bar: **https://portal.office.com**
12. In the **Sign in** window, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
13. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
14. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
15. This opens the **Microsoft Office Home** tab in your InPrivate browsing session. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketin**
16. This opens the **Marketing** site collection. In the upper-right corner of the screen (to the left of the circle with the **MA** initials), select the **gear (Settings)** icon (the wheel icon). In the **Settings** window that appears, select **Site settings**.
17. On the **Site Settings** page, under the **Users and Permissions** group, select **Access requests and invitations**.
18. On the **Access requests** page, verify that Joni Sherman's request appears under the **Pending Requests** section. For Joni's request, select the **Approve** button.
19. On the current **Access Requests - Default** tab, select the back arrow on the address bar to return to the **Site Settings** page. Under the **Users and Permissions** group, select **Site permissions**.
20. On the **Site permissions** page, in the list of users who have access to this site, select **Marketing Members**.
21. In the **People and Groups - Marketing Members** page, verify that Joni Sherman's account appears in the list.
22. You now want to invite Nestor Wilke to become a member of the Marketing Site Collection. On the menu bar at the top of the page, select the drop-down arrow to the right of **New**, and then in the drop-down menu that appears, select **Add Users**.

23. On the **Share 'Marketing'** window, the **Invite People** tab is displayed by default. In the **Enter names or email addresses** field, enter **Nestor**. A list of users whose first name starts with Nestor will appear. Select **Nestor Wilke** and then select **Share**.

    Nestor's name will now appear in the **People and Groups - Marketing Members** page along with Joni Sherman.

24. Close this InPrivate browsing session for the **MOD Administrator**.
25. You will now verify whether Joni Sherman can access the the Marketing site. Perform the same steps as before to open a new **InPrivate** browsing session.
26. In your new **InPrivate** browsing session, enter the following URL in the address bar: **https://portal.office.com**
27. In the **Sign in** window, enter **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
28. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
29. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
30. This opens the **Microsoft Office Home** tab in your InPrivate browsing session. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketin** (where ZZZZZZ is the tenant ID provided by your lab hosting provider).
31. This opens the **Marketing** site collection. You have just verified that Joni can access the site after requesting access to it and later being granted access by a site administrator.
32. Close this InPrivate browsing session for **Joni Sherman**.
33. You will now verify whether Nestor Wilke can access the the Marketing site. Perform the same steps as before to open a new **InPrivate** browsing session.
34. In your new **InPrivate** browsing session, enter the following URL in the address bar: **https://portal.office.com**
35. In the **Sign in** window, enter **NestorW@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
36. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
37. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
38. This opens the **Microsoft Office Home** tab in your InPrivate browsing session. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketin** (where ZZZZZZ is the tenant ID provided by your lab hosting provider).
39. This opens the **Marketing** site collection. You have just verified that Nestor can access the site after the site admin (the MOD Administrator) shared site membership with him.
40. Close this InPrivate browsing session for **Nestor Wilke**.
41. Leave your Edge browsing session open along with all its tabs.

Results: After completing this exercise, you should have created and configured SharePoint Online site collections.

38 Proceed to Lab 9 - Exercise 3

39 Module 9 - Lab 9 - Exercise 3 - Configuring and verifying external user sharing

In the last two exercises, Holly Dickson has configured SharePoint Online services and SharePoint Online site collections. She is now ready to configure SharePoint Online for external sharing as part of her overall permissions planning for SharePoint in Microsoft 365.

The external sharing features of Microsoft SharePoint let users in an organization share content with people outside the organization (such as partners, vendors, clients, or customers). External sharing can also be used

to share between licensed users on multiple Microsoft 365 subscriptions if your organization has more than one subscription.

SharePoint has external sharing settings at both the organization level and the site collection level. To allow external sharing on any Adatum site, Holly must first allow it at the organization level. She can then restrict external sharing for other sites. If a site's external sharing option and the organization-level sharing option don't match, the most restrictive value will always be applied.

Even if your organization-level setting allows external sharing, not all new sites allow it by default. The default sharing setting for Microsoft 365 group-connected team sites is "New and existing guests." The default for communication sites and classic sites is "Only people in your organization."

In this exercise, Holly will allow external sharing at the organization level and for a specific site collection. She will then verify that she can share a document as well as a site within the site collection with external users.

39.1 Task 1: Configure global settings for external user sharing

In this task, Holly will enable external sharing at the organization level. The sharing feature that she wants to enable is in the SharePoint classic admin center and not the new SharePoint admin center.

1. You should still be on **LON-CL1**, where you should be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. You should still have Microsoft Edge open from an earlier lab, along with tabs for the **Microsoft Office Home** page, **Microsoft 365 admin center**, and **SharePoint admin center**.

   If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and **Pa55w.rd**, and then in the **Microsoft Office Home** page, select **Admin**, and then in the **Microsoft 365 admin center**, select **SharePoint**.
3. On the **SharePoint admin center**, in the left-hand navigation pane, select **Policies** and then select **Sharing**.
4. On the **Sharing** page, verify the **Allow only users in specific security groups to share externally** check box is not selected, in which case you can close this **Sharing** window. If this check box is selected, then unselect it and select **Save**.
5. Leave all tabs open in your browser and proceed to the next task.

39.2 Task 2: Configure a site collection for external user sharing

In the prior lab exercise, you created a new Marketing site collection. In this task, you will configure it to allow external sharing.

1. You should still be on **LON-CL1**, where you should be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. You should still have Microsoft Edge open from an earlier lab, along with tabs for the **Microsoft Office Home** page, **Microsoft 365 admin center**, and **SharePoint admin center**.
3. In the **SharePoint admin center**, in the left-hand navigation pane, select **Sites** and then select **Active sites**.
4. On the **Active sites** page, in the list of sites, select the **Marketing** site.
5. In the **Marketing** pane that appears on the right side of the screen, select the **Policies** tab.
6. In the **Policies** tab, under the **External sharing** group, select **Edit**.
7. On the **Sharing** window that appears, under the **External sharing** group, the **Anyone** option should be selected by default.

   If this option is not selected, then select it now and select **Save**. If the **Anyone** option was already selected, then close the **Sharing** window.
8. Close the **Marketing** pane.

9. You must now open an In-Private browsing session for the MOD Administrator to access the new Marketing site. Right-click on the **Edge** icon on the taskbar, and in the menu that appears, select **New InPrivate window**.
10. In your **InPrivate Browsing** session, enter the following URL in the address bar: **https://portal.office.com**.
11. In the **Sign in** window, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and then select **Next**.
12. In the **Enter password** window, enter (or copy and paste in) the tenant admin password provided by your lab hosting provider and then select **Sign in**.
13. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
14. This opens the **Microsoft Office Home** tab in your Edge browser. Open a new tab in your browser and enter the following URL in the address bar: **https://M365xZZZZZZ.sharepoint.com/sites/Marketing** (where ZZZZZZ is the tenant ID provided by your lab hosting provider).
15. In the **Marketing** site, in the top-right corner, select **SHARE**.
16. In the **Share 'Marketing'** window, you can see that the site is currently shared with Nestor Wilke, Joni Sherman, and Patti Fernandez.
17. On the **Share 'Marketing'** window, the **Invite People** tab is displayed by default. In the **Enter names or email addresses** field, enter your personal email address. Your email address will appear in a list below this field; select this address now.

    Your email addres will appear below this field, along with a message indicating it is outside of Adatum's organization.
18. In the **Include a personal message with this invitation (optional)** field, enter the following message: **You can now access the SharePoint site collection for Adatum's Marketing team.**
19. Select **Share**.
20. On the **Marketing** page, in the left-hand navigation pane, select **Documents**.
21. On the **Documents** page, in the menu bar, select **+New**, and then in the drop-down menu that appears, select **Word document**.
22. **Word Online** will open in a new tab in your browser. In the **Your privacy option** window that appears, select **Close**.
23. In the blank **Word** document, type some text, and then wait for the document to be automatically saved. Once it is saved, the word **Saved** will appear in the document title. Once the document is saved, select the drop-down arrow that appears to the right of **Saved**. In the drop-down menu that appears, in the **Location** field, the path **Marketing - Shared Documents** appears (where each is hyperlinked). Select the **Shared Documents** link.
24. This will open the **Marketing** site and the **Documents** tab. In the **Documents** page, the document that you just created (Document.docx, since you did not name it), should appear in the documents list.
25. In the document list, select the vertical ellipsis icon to the right of the document name, and in the menu that appears, select **Share**.
26. In the **Send link** window that appears, select **Anyone with the link can edit**.
27. In the **Link settings** window that appears, under the **Who would you like this link to work for?** section, select **Anyone with this link** and then select **Apply**.
28. In the **Send link** window, in the **Enter a name or email address**, enter your personal email address, and enter **This document is shared with you. You have edit permissions.** in the **Add a message (optional)** field. Select **Send**.
29. Close the **Link sent** window that appears.
30. Select **Close**.
31. Close the InPrivage browsing session for the **MOD Administrator**.
32. Leave all tabs open in your browser and proceed to the next task.

39.3 Task 3: Verify external user sharing

1. Navigate to your personal email maibox.
2. The Inbox should include two emails from Microsoft Online Services Team. If the messages are not in the Inbox, look in the Junk folder.
3. Open the message that has the subject: **MOD Administrator wants to share Marketing**.
4. Select the **Marketing** link in the email.
5. Select either **Microsoft Account** or **Organizational Account** depending the email account type and verify that you can access the **Marketing** site. Select the **Documents** tab and verify you can access the shared document.
6. In your Inbox, open the second invitation email message with the subject of **MOD Administrator wants to share the document**.
7. Select the **Document** link.

   Note: You are redirected directly to the Word Document. Word Online opens and displays the document.
8. Verify that you can access the Word document and then select **Edit in Browser**.
9. Add some text in this document. Close the document and then re-open it to verify your changes appear.
10. On the **Microsoft Office Home** page, select the user icon (the circle with Holly Dickson's **HD** initials in it) in the upper right-hand corner, and in the **My account** window that appears, select **Sign out**. Once you are signed out, close all other tabs, and then close Microsoft Edge.

Results: After completing this exercise, you should have configured a new site collection for external user sharing, and you should have shared a site and a document with external users.

40 End of Lab 9

41 Module 10 - Lab 10 - Exercise 1 - Configuring Yammer Enterprise

Because Yammer Enterprise brings the rich social experiences of Yammer to Microsoft Teams, SharePoint Online, and other Microsoft 365 apps, Holly Dickson is interested in implementing Microsoft Yammer in Adatum's Microsoft 365 pilot project. This will enable Adatum users to share, create, and edit files directly from Yammer conversations with Office for the web.

In this exercise Holly will configure the Yammer organizational settings for Adatum. She will also configure Yammer to enforce Microsoft 365 identity, which enables single sign-on (SSO) capabilities in Yammer. Holly will complete her Yammer preparation by configuring the Yammer user experience.

41.0.1 Task 1 - Configure a Yammer organization setting

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. At the end of the prior lab, you were instructed to sign out of Microsoft 365 as Holly Dickson and close your Microsoft Edge browsing session. If you did not do it, then please do so now. This will enable you to start with a fresh browsing session.

   With Edge closed, select the **Edge** icon on the taskbar to open a new session.
3. In Edge, enter the following URL in the address bar: **https://portal.office.com**.
4. In the **Pick an account** window, select Holly Dickson's account (**Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider)). In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
5. On the **Stay signed in?** window, select **Don't show this again** and then select **Yes**.
6. On the **Microsoft Office Home** page, select **Yammer**.
7. On the **Yammer** home page, on the right-side of the title bar at the top of the page, select the **gear (Settings)** icon.
8. In the **Settings** pane that appears, under the **Yammer** section, select **Edit network admin settings**. This opens the **Yammer admin center**.

9. In the **Yammer admin center**, in the left-hand navigation pane, under the **Network** group, select **Usage Policy**.
10. In the **Usage Policy** window, update the following settings:
    - Select the **Require users to accept policy during sign up and after any changes are made to the policy** check box.
    - Select the **Display policy reminder in sidebar** check box.
    - In the **Custom Policy Title** field, enter**M365x Acceptable Use Policy**.
    - In the **Enter your policy in the textbox below** field, copy and paste in the following text: **Welcome to Yammer! Our goal is to provide a collaborative environment to connect with colleagues and bridge various departments and geographic locations to share meaningful information.**
11. Select **Save**.
12. In the **M365x Acceptable Use Policy** window that appears, select **I Accept**.
13. In the **Welcome to the new Yammer!** window, select the X in the upper right corner to close it.
14. On the **Yammer** home page, on the right-side of the title bar at the top of the page, select the **gear (Settings)** icon.
15. In the **Settings** pane that appears, under the **Yammer** section, select **Edit network admin settings**. This opens the **Yammer admin center**.
16. In the **Yammer admin center**, in the left-hand navigation pane, under the **Network** group, select **Configuration**.
17. On the **Configuration** page, in the **Email Settings** section, select the **Require all users in your network to confirm their messages posted via email before posting** check box.
18. In the **Enabled Features** section, remove the check mark from **3rd Party Applications** to disable this feature.
19. Select **Save**.
20. In the **Yammer admin center**, in the left-hand navigation pane, under the **Content and Security** group, select **Data Retention**.
21. In the **Data Retention Policy** page, read the description of available options and select **Archive** (if it's not already selected) and then Select **Save**.
22. In the **Yammer admin center**, in the left-hand navigation pane, under the **Content and Security** group, select **Monitor Keywords**.
23. In the **Monitor Keywords** page, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) in the **Email Address** field.
24. In the text box below the **Email Address** field, enter the following words, one in each line: **gambling**, **erotic**, **warez**.
25. Select **Save**.
26. In the **Yammer admin center**, in the left-hand navigation pane, under the **Content and Security** section, select **Security Settings**.
27. Under the **Office 365 Identity Enforcement** section, verify the **Enforce Office 365 identity** check box is selected by default and then select **Save**.
28. In your Edge browser, close the **Yammer admin center** tab and proceed to the next task.

41.0.2 Task 2 - Configure the Yammer user experience

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. At the end of the prior task, you were instructed to close the **Yammer admin center** tab. If you did not do it, then please do so now.
3. In your Edge browser, you will re-open Yammer to start a fresh session with the updated configuration settings from the prior task. On the **Microsoft Office Home** page, select **Yammer**.

4. On the **Yammer** home page, on the right-side of the title bar at the top of the page, select the **gear (Settings)** icon.
5. In the **Settings** pane that appears, under the **Yammer** section, select **Edit settings**. This opens the **Account Settings** page.
6. the **Account Settings** page, select the **Notifications** tab at the top of the page.
7. In the list of notifications, all the check boxes in the **Email me when...** section are selected. Unselect all the check boxes except for these three:
   - **I receive a message in my inbox**
   - **I log in from somewhere new**
   - **I post a message via email (This will send a confirmation email)**

   Verfify that only these three check boxes are selected and all other check boxes are now blank.
8. Select **Save**.
9. Leave your Edge browsing session open, but close the **Yammer: Notifications** tab and proceed to the next task.

41.0.3 Task 3 - Using Yammer

In this task, you will log into Yammer as Nestor Wilke and verify that you receive the Acceptable Use Policy statement that Holly configured in the earlier task.

1. Switch to **LON-CL2**. The last time you used LON-CL2, you were logged into Outlook on the web as the MOD Administrator. You were then instructed to log out of Outlook and close your Edge browsing session at the end of the lab. If your Edge browser is still open, then close it now.
2. Select the **Microsoft Edge** icon on the taskbar to open a new Edge browsing session, and then enter the following URL in the address bar: **https://portal.office.com**.
3. In the **Pick an account** window, if Nestor Wilke's **NestorW@M365xZZZZZZ.onmicrosoft.com** account appears in the list, then select it now; otherwise, select **Use another account**, sign in as **NestorW@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider), and enter (or copy and paste in) the tenant admin password provided by your lab hosting provider.
4. On the **Microsoft Office Home** page, select **Yammer**.
5. If a **Welcome to the new Yammer!** window appears, then close it.
6. A **M365x Acceptable Use Policy** dialog box should appear that displays the Welcome message that Holly configured in the earlier task. Select **I accept**.

   You have now verified that a user who is signing into Yammer for the first time receives the Acceptable Use Policy statment. If Nestor were to sign out of Yammer and then sign back in, the **M365x Acceptable Use Policy** dialog box would not appear, since he already accepted it.

Results: After completing this exercise, you should have enabled Yammer Enterprise for ADatum Corporation.

42 Proceed to Lab 10 - Exercise 2

43 Module 10 - Lab 10 - Exercise 2 - Configuring OneDrive for Business

Now that she has implemented Microsoft Yammer in Adatum's Microsoft 365 pilot project, Holly Dickson is ready to do the same with Microsoft OneDrive for Business. Holly knows that with OneDrive, Adatum's users can easily and securely store and access their files from all their devices. This will enable them to more efficiently work with others regardless of whether they're inside or outside the organization and terminate that sharing whenever they want.

Holly also knows that OneDrive for Business will help protect their work through advanced encryption while the data is in transit and at rest in data centers. Because Adatum is serious about improving its security requirements, Holly plans to implement OneDrive to help ensure that her users adhere to Adatum's most rigorous

compliance standards by enabling them to choose where their data lives and providing detailed reporting of how that data has been changed and accessed.

In this exercise, Holly will enable OneDrive for Business synchronization, create test files to be synchronized, and then verify file synchronization.

This lab exercise will be performed within LON-CL2.

43.1 Task 1: Enable OneDrive for Business synchronization

1. On **LON-CL2**, you should still be logged in as the **Administrator**.
2. If Microsoft Edge is open from an earlier lab, then close it now.
3. In an earlier lab, you logged into Microsoft 365 as Alan Yoo and you downloaded and installed **Microsoft 365 Apps for enterprise**.

   You should now open your local **Word** app again by selecting the **Windows** icon on the bottom-left corner of the taskbar, and then in the **Start** menu, selecting **Word**.
4. When **Word** opens, verify which user account it is licensed to at the top of the Word document. If Alan's name appears along with his initials in a circle, then skip to the next step.

   However, if a different user account appears, then select the user account, and in the window that appears, select **Sign in with a different account**. In the **Sign in** window, enter **alan@M365xZZZZZZ.onmicrosoft.com (where ZZZZZZ is the unique tenant ID provided by your lab hosting provider) and a password of **Pa55w.rd**. Verify that **Alan Yoo** now appears at the top of the Word form.
5. Now that you have verified that Word is licensed to Alan Yoo, close Word.
6. Open Microsoft Edge and then connect to **https://portal.office.com**.
7. Sign in as **Alan@M365xZZZZZZ.onmicrosoft.com** with a password of **Pa55w.rd**.
8. On the **Microsoft Office Home** page, select **OneDrive**.
9. If the **Welcome to OneDrive for Business** page appears, Select **Next**.
10. In the **OneDrive** window, select **+New** at the top of the page, and then in the drop-down menu that appears, select **Word document**.
11. If a **Your privacy option** window appears, select **Close**.
12. In the **Word Online** tab that opens in your Edge browser, type some text, at which point Word Online will save the document as **Document.docx**.
13. You want to rename the document as **OneDrive Test**, so in the Word menu bar, select **File**, select **Save as**, and then select **Rename**. In the window that appears, enter **OneDrive Test** in the **File Name** field and then select off this field. This will change the file name and close the window.
14. Close the Word Online tab in your browser.
15. In the **OneDrive** window, the **OneDrive test.docx** file should now appear in the list of files. On the menu bar at the top of the page, select **Sync**.
16. In the **This site is trying to open Microsoft OneDrive** window, select the **Always allow m365xZZZZZZ-my.sharepoint.com to open links of this type in the associated app** check box and then select **Open**.
17. In the **Set up OneDrive** window, Alan Yoo's account is displayed in the username field. Select **Sign in**.
18. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
19. In the **Your OneDrive folder**, note the location of your OneDrive folder and then select **Next**.
20. On the **Sync your files to this PC** window, select **Next**.
21. On the **Get to know your OneDrive** window, select **Next**.
22. On the **Share files and folders** window, select **Next**.
23. On the **Get the mobile app** window, select **Later**.
24. On the **You OneDrive is ready for you** window, select **Open my OneDrive folder**.

25. **File Explorer** is automatically opened for you. In the **File Explorer** window, select **OneDrive - Adatum Corporation**.
26. Note that File Explorer displays the location where the synchronized files will be stored. Verify that the **OneDrive test.docx** file that you created earlier in Word Online has been synchronized to the local computer.
27. Leave File Explorer open as well as your Edge browser and proceed to the next task.

43.2 Task 2: Create files to synchronize with OneDrive for Business

Now that you have enabled file synchronization with OneDrive for Business, Holly Dickson wants to create test files to be synchronized and then verify file synchronization.

1. On **LON-CL2**, ensure that the **OneDrive for Business** folder is open in File Explorer from the previous task. If not, open **File Explorer** and select **OneDrive - Adatum Corporation**.
2. In **File Explorer**, select **Home** that appears in the menu bar at the top of the window.
3. In the ribbon that appears on the **Home** tab, select **New folder**. This creates a new folder. Enter **Private** as the folder name.
4. You now want to create another folder, so select the **Home** tab again, and on the ribbon, select **New folder**, and then enter **Project A** as the folder name.
5. You now want to create a new Word document in the **Private** folder.

   If you double-click on the **Private** folder and then right-click in the detail pane and select **New** in the menu, it does NOT provide an option to create a Microsoft Word document.

   Instead, in the folder tree in the left-hand pane of the File Explorer window, you must select **OneDrive - Adatum Corporation** to expand it, then select the **Private** folder, right-click in the detail pane, and then select **New** in the menu. This will display a sub-menu with a variety of file types. Select **Microsoft Word Document** and name the document **Holidays.docx**.
6. In the **File Explorer** window, note the document icon that appears to the left of the **Holidays.docx**. It may be hard to see, but the icon is an image of two blue arrows. This will come into play after you complete this step.

   Double-click the **Holidays.docx** to open it (note Alan Yoo is the licensed user displayed in the top left-corner of the Word document). Type some text in the document, save the document, and then close Microsoft Word.
7. Note how the document icon for **Holidays.docx** changes from two blue arrows to a small green check mark icon after the synchronization process is complete. The document has been transferred to the OneDrive cloud storage automatically.
8. In the **File Explorer** window, navigate to **OneDrive for Business** in the navigation address line to move one level up.
9. In the **File Explorer** window, with the **OneDrive - Adatum Corporation** object expanded in the folder tree, select the **Project A** folder. Right-click in the detail pane for this folder, and in the menu that appears, select **New**, and then select **Microsoft Word Document**. Name the document **Project targets.docx**.
10. Double-click **Project targets.docx** to open it, and then type some short text, save the changes, and then close Microsoft Word.
11. Verify that the document synchronized by checking the document icon in File Explorer. The icon should be a green check mark.
12. Minimize the **File Explorer** window.
13. To view the files online, switch to the Microsoft Edge window. You should still be in the **OneDrive** tab. Refresh the view.
14. In the **Files** list, you should see your two folders - **Private** and **Project A**.
15. Select the **Private** folder, and then select the **Holidays.docx** file to open it in Word Online.

16. In the menu bar at the top of the page, the **Tell me what you want to do** option is set to **Editing**. Add some additional text to the document. The document is saved automatically when **Saved** is displayed in the title bar.
17. In your Edge browser, select the **OneDrive for Business** tab.
18. Since you just updated the **Holidays.docx** file, you will see this reflected in the **Modified** column, which shows that the document changed just a few seconds ago.
19. Switch back to **File Explorer**.
20. In the folder tree, **OneDrive - Adatum Corporation** should still expanded. Select the **Private** folder and then open **Holidays.docx**. You should see the changes you made in Word Online are synchronized back automatically.
21. Leave File Explorer open as well as your Edge browser and proceed to the next task.

43.3 Task 3: Share files with other users

1. On **LON-CL2**, ensure that the **OneDrive for Business** folder is open in File Explorer from the previous task. If not, open **File Explorer** and select **OneDrive - Adatum Corporation** to expand it so that you can see the **Private** and **Project A** folders.
2. In **File Explorer**, in the folder tree under **OneDrive - Adatum Corporation**, right-click the **Project A** folder and select **View online**.
3. Microsoft Edge opens (if you receive a dialog box asking which app to use to open this folder, select Microsoft Edge). If you are prompted to sign in, then sign in as Alan Yoo (**alan@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your tenant ID)) and a password of **Pa55w.rd**.
4. In your Edge browser, a tab should open with Alan Yoo's **OneDrive for Business** account. The tab should be displaying Alan's **My Files**, and specifically the **Project A** folder.

   Hover your mouse to the left of the **Project Targets.docx** field and select the circle so that it displays a check mark. With the file selected, select **Share** that appears in the menu bar at the top of the page..
5. In the **Send link** window that appears, enter the following information:
   - Enter **MOD** in the **Enter a name or email address** field. This will return a list of users whose name starts with MOD. Select **MOD Administrator**.
   - In the **Add another** field, enter **Patti**. In the list of users, select **Patti Fernandez**.
   - In the **Add a message (optional)** field, enter **This is the latest information for Project A**.
6. Select **Send**. After the emails are created, close the **Link sent** window.
7. In the upper text box, type **MOD Administrator**.
8. Open a new InPrivate Microsoft Edge window, and then connect to **https://portal.office.com**.
9. Sign in as **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID) and copy and paste in the tenant password provided by your lab hosting provider.
10. In the **Microsoft Office Home** page, select **Outook**.
11. Select the message with the subject **Alan Yoo shared ""Project Targets" with you**.
12. In the message box, select **Project Targets**.
13. Verify the document opens, and then make some changes to it. The changes should be automatically saved, and the file name at the top of the document should display **Saved**. All modifications are stored online in the OneDrive for Business cloud storage. By default, SharePoint Online creates a new version when the document changes. This can be viewed by the owner in the version history.
14. Close the InPrivate Microsoft Edge window.
15. You now want to turn off sharing for this document. In the Microsoft Edge window, the **Project targets** document should still be selected. Note in the file list, the **Sharing** column indicates the file is **Shared**.

    Select the **Shared** status in the **Sharing** column. This will open a **Manage access** window. (Note - Nother way to open the **Manage access** window for this file is to select **Share** in the menu bar just as you did when you originally shared the file, and then select the ellipsis icon in the **Share** window, and then select **Manage access**).

16. In the **Manage access** window, select **Stop sharing**. In the confirmation window that appears, select **Stop sharing** again.
17. Close the **Manage Access** window. Note in the file list how the value of the **Sharing** column for this file changed from **Shared** to **Private**.
18. On the **Microsoft Office Home** page, select the user icon (the circle with Alan Yoo's **AY** initials in it) in the upper right-hand corner, and in the **My account** window that appears, select **Sign out**. Once you are signed out, close all other tabs, and then close Microsoft Edge.

Results: After completing this exercise, you should have configured Microsoft OneDrive for Adatum.

44 Proceed to Lab 10 - Exercise 3

45 Module 10 - Lab 10 - Exercise 3 - Configuring Microsoft 365 groups

Holly Dickson is ready to finalize user collaboration in Microsoft 365 by implementing Microsoft 365 groups, which help in collaboration and teamwork, are available across all Microsoft 365 services, and are highly integrated with all Microsoft 365 services. Microsoft 365 groups, which are part of Azure Active Directory, are only available in Microsoft 365. Each Microsoft 365 group has a mailbox, a calendar, a Microsoft OneNote notebook, and a OneDrive for Business site collection.

In this exercise, Holly will configure a private Microsoft 365 group through the Microsoft 365 admin center. For comparison purposes, she will then create a public group through Windows PowerShell. She will complete this process by exploring the Microsoft 365 group components.

45.0.1 Task 1 - Configure a private Microsoft 365 group

1. Switch to **LON-CL1**, where you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. In the previous lab exercise involving Microsoft Yammer, you logged into Microsoft 365 as Holly Dickson. In your Edge browser, you should still have a tab open for the **Microsoft Office Home** page. In the the **Microsoft Office Home** page, select **Admin** to open the **Microsoft 365 admin center**.
3. In the **Microsoft 365 admin center**, select **Groups** in the left navigation pane and then select **Active groups**.
4. In the **Active Groups** window, select **Add a group** on the menu bar at the top of the page.
5. In the **Choose a group type** pane that appears, the **Microsoft 365** group type is selected by default. Accept this value by selecting **Next**.
6. In the **Set up the basics** window, enter **Finance** in the **Name** field and **Collaboration group for the Finance team** in the **Description field** and then select **Next** (Note - if you leave the **Description** field blank, you must still select it to enable the **Next** button).
7. In the **Assign owners** window, enter **MOD** in the **Owners** field, which will display the list of active users whose first name starts with MOD. Select **MOD Administrator** and then select **Next**.
8. In the **Edit settings** window, enter **Finance** in the **Group email address** field.

   Note: To the right of the **Group email address** field is the domain field. It's already prefilled with the **M365xZZZZZZ.onmicrosoft.com** domain, which is set as Adatum's Default domain. This is different from adding users in that no other domains appear; therefore, you must leave this value as is.

   After configuring this field, the Finance group email address should appear as: **Finance@M365xZZZZZZ.onmicrosoft.com**

   After configuring the email address, under the **Privacy** section, select **Private**, and leave the check box selected to **Create a team for this group**. Select **Next**.
9. On the **Review and finish adding group** window, review the information and if anything needs to be changed, select the appropriate **Edit** option; otherwise, select the **Create group** button at the bottom of the page.

10. On the **New group created** window, note the message that appears at the top of the page that indicates it may take up to 5 minutes before the group appears in the list of active groups. Select **Close**
11. On the **Active groups** window, select **Refresh** on the menu bar to refresh the list of active groups. You may have to wait a few minutes and refresh again. Once the **Finance** group appears in the list, select the group.
12. In the **Finance** pane that appears, the **General** tab is displayed by default. Select the **Members** tab.
13. In the **Members** tab, under the **Members** group, select **View all and manage members**.
14. In the **Finance** group window, select **+Add members**. This displays the list of current users.
15. In the list of users, select **Joni Sherman** and then select **Save**.
16. Select **Close**. This displays the list of users for this group. Select **Close** again.
17. On the **Finance** window, select the **X** in the upper right-hand corner to close the window.
18. Leaver your Edge browser and all its tabs open and proceed to the next task.

45.0.2 Task 2 - Configure a public Microsoft 365 group with Windows PowerShell

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. Back in Lab 2, you installed the **Windows Azure Active Directory Module for Windows PowerShell**. If you still have Windows PowerShell open, then select it now on the taskbar; otherwise, open an elevated instance of **Windows PowerShell** (i.e. Run as administrator).
3. In **Windows PowerShell**, at the command prompt type the following command and then press Enter to store your administrative credentials as a macro ($cred):

   ```
   $cred = Get-Credential
   ```

4. In the **Windows PowerShell credential request** window, sign in as **admin@M365xZZZZZZ.onmicrosoft.com** (replace ZZZZZZ with the tenant ID provided by your lab hosting provider) and then enter (or copy and paste in) the tenant admin password provided by your lab hosting provider.
5. At the command prompt type the following command and then press Enter to create a session with Microsoft Exchange Online:

   ```
   $session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.off
   ```

6. At the command prompt type the following command and then press Enter to import the session into the PowerShell console (Ignore the warning message that is generated):

   ```
   Import-PSSession $Session -AllowClobber
   ```

7. At the command prompt type the following command and then press Enter to create a new public Microsoft 365 group called Planning (replace ZZZZZZ with the tenant ID provided by your lab hosting provider):

   ```
   New-UnifiedGroup -DisplayName "Planning" -Alias "Planning" -EmailAddresses Planning@M365xZZZZZZ.o
   ```

8. At the command prompt type the following command and then press Enter to add the MOD Administrator as the owner for the group (replace ZZZZZZ with the tenant ID provided by your lab hosting provider):

   ```
   Add-UnifiedGroupLinks "Planning" -Links Admin@C -LinkType Owner
   ```

9. At the command prompt type the following command and then press Enter to add Ada Russell as a member of the group (replace ZZZZZZ with the tenant ID provided by your lab hosting provider):

   ```
   Add-UnifiedGroupLinks "Planning" -Links Ada@M365xZZZZZZ.onmicrosoft.com -LinkType Member
   ```

10. Minimize the Windows PowerShell window and proceed to the next task.

45.0.3 Task 3 - Explore the Microsoft 365 group components

In this task, you will log into Microsoft 365 as the MOD Administrator, who is the owner of the Planning group. You will then see how the Planning group is accessible to the MOD Administrator in Outlook, since the MOD Administrator is an owner of this group. You will send an email from the MOD Administrator to the Planning group. You will also send a meeting request from the Planning group to Joni Sherman. You will then create a document for the Planning group. Finally, Joni Sherman will join the Planning group and verify that received

the email from the MOD Admin to the Planning group, and that she can access the document created for the group.

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. In your Edge browser, you should still be logged into Microsoft 365 as Holly Dickson. Sign out of Microsoft 365 as Holly, close all your browser tabs except for your sign out tab, and then navigate to **https://portal.office.com**. Log in as the **MOD Administrator (admin@M365xZZZZZZ.onmicrosoft.com)** with the tenant admin password.
3. On the **Microsoft Office Home** tab, select **Outlook**.
4. In **Outlook**, scroll to the bottom of the folder list in the left-hand pane. Under the **Groups** section, select **Planning**.
5. In the **Planning** pane that appears, select **Send email**.
6. In the message window, the Planning group is prefilled in the **To** field. Enter a subject and some text in the message and then select **Send**.
7. In the **Planning** pane, select the **calendar (Go to the group calendar)** icon that appears to the right of **Send email** the you previously selected. This will open a new tab in your browser and take you to the Planning group's calendar.
8. In the **Planning group's calendar**, select **New event**. In the **Details** pane for this event, type **Planning group meeting** for the title, schedule it for tomorrow, and then select **Save**.
9. Close the tab for the Planning group's calendar.
10. In your Edge browser, in the **Mail - MOD Administrator** tab, select the calendar icon. Ensure the Planning group's calendar synchronizes with the Admin's personal calendar.
11. In **Outlook**, scroll to the bottom of the folder list in the left-hand pane. Under the **Groups** section in the left-hand pane, select **Planning** once again.
12. In the **Planning** pane, select the **file (Go to the group files)** icon that appears to the right of **Send email** the you previously selected.
13. In the **Documents** window for the Planning group, select **+New** in the menu bar at the top of the form. In the drop-down menu that appears, select **Word document**.
14. In Word Online, type some text into the blank document. When you see **Saved** in the title bar, select **File** in the menu bar, select **Save as**, and then select **Rename**. In the **File name** window, enter **Planning Review** as the name of the document. Select the document and note the change to the file name at the top of the form.
15. Close the Word Online tab in your Edge browser.
16. In the **Planning** group pane, if the original document name (**Document.docx**) appears in the list of files rather than the new name you assigned, select the **Refresh** icon to the left of the address bar. Once the Planning group's Files page refreshes, you should see the renamed document.
17. On LON-CL1, open a **New InPrivate Browsing** window in Microsoft Edge. You will log into Microsoft 365 as Joni Sherman. Because the **Planning** group is a Public group, Joni can add herself to the group.
18. In the new **InPrivate** browsing window, enter **https://portal.office.com** in the address bar and then sign in as **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and the enter (or copy and paste in) the tenant admin's password provided by the lab hosting provider.
19. In the **Microsoft Office Home** page, select **Outlook**.
20. In **Outlook**, scroll to the bottom of the folder list in the left-hand pane. Locate the **Groups** section, then right-click on **Groups** and in the menu that appears select **Discover groups**.
21. In the **Discover groups** window, enter **Planning** in the **Search for groups** field and then press Enter to search for the group.
22. The search should return the **Planning** group. Select the **Join** button. Once the **Join** button changes to **Joined group**, close the **Discover groups** window.

23. In **Outlook**, in the folder pane on the left, the **Planning** group should now appear under the **Groups** section. Select the **Planning** group.
24. Verify that the email from the MOD Administrator to the Planning group appears.
25. Select the **Go to group files** icon.
26. On the **Files** page, verify the **Planning Review.docx** file appears. This is the document the MOD Administrator created for the Planning group.
27. Close the InPrivate browsing session for Joni Sherman.
28. On the **Microsoft Office Home** page, select the user icon (the circle with MOD Administrator's **MA** initials in it) in the upper right-hand corner, and in the **My account** window that appears, select **Sign out**. Once you are signed out, close all other tabs, and then close Microsoft Edge.

Results: After completing this exercise, you should have configured Microsoft Microsoft 365 groups at Adatum.

46 End of Lab 10

47 Module 11 - Lab 11 - Exercise 1 - Creating Sensitivity Labels

Adatum has transitioned to Microsoft 365 as its enterprise cloud solution. The company has been awarded several government contracts which work heavily with sensitive and classified products.

In your role as Holly Dickson, Adatum's Enterprise Administrator, the company CTO has requested that you devise a solution for encrypting and securing messages when working in these related contracts. He has also requested that any references to "Project New Day" be automatically encrypted. This is a top-secret project, and it is imperative that no mention of this project be leaked outside the company.

In this lab, you will address your CTO's request by creating sensitivity labels that will be used for creating label policies. You will create sensitivity labels using the Microsoft 365 Security center as well as Windows PowerShell. While still satisfying your CTO's request, this plan will provide you with experience using each method as part of your pilot project. This way, you can later decide which approach you prefer when you transition from your pilot phase to the production phase. With your labels in place, you will then create a label policy - again, using both the Security center and PowerShell.

Important: Sensitivity labels and policies can take up to 24 hours to propagate through the system and update the back-end servers. Unfortunately, with this training course nearing its end, you will not have time to verify your work by testing the labels and policies you created. However, it is hoped that this lab exercise will still provide you with experience and insight into the mechanics of creating sensitivity labels and policies, even though you cannot test them.

47.0.1 Task 1 - Creating a test team

In your role as Holly Dickson, you will create a new Microsoft 365 group titled PND Group (for Project New Day, the name of which you want to avoid circulating through the company) that will be used as part of your sensitivity label testing in the upcoming tasks.

1. In **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. At the end of the prior lab, you logged out of Microsoft 365 as the MOD Administrator and closed Edge. Select the **Edge** icon on the taskbar and then enter the following URL in the address bar: **https://portal.office.com**.
3. In the **Pick an account** window, select **Holly Dickson** at **holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant ID provided by your lab hosting provider) and enter **Pa55w.rd** as her password.
4. On the **Microsoft Office Home** page select **Admin**.
5. On the **Microsoft 365 admin center**, in the left-hand navigation pane select **Groups**, and then select **Active groups**.
6. In the **Active Groups** window, select **Add a group** on the menu bar at the top of the page.
7. In the **Choose a group type** pane that appears, the **Microsoft 365** group type is selected by default. Accept this value by selecting **Next**.

8. In the **Set up the basics** window, enter **PND Group** in the **Name** field and **Group used for sensitivity label testing** in the **Description field** and then select **Next** (Note - if you leave the **Description** field blank, you must still select it to enable the **Next** button).
9. In the **Assign owners** window, enter **MOD** in the **Owners** field, which will display the list of active users whose first name starts with MOD. Select **MOD Administrator** and then select **Next**.
10. In the **Edit settings** window, enter **PNDgroup** in the **Group email address** field.

    Note: To the right of the **Group email address** field is the domain field. It's already prefilled with the **M365xZZZZZZ.onmicrosoft.com** domain, which is set as Adatum's Default domain. This is different from adding users in that no other domains appear; therefore, you must leave this value as is.

    After configuring this field, the PND Group email address should appear as: **PNDgroup@M365xZZZZZZ.onmicrosoft.com**

    After configuring the email address, under the **Privacy** section, select **Private**, and leave the check box selected to **Create a team for this group**. Select **Next**.
11. On the **Review and finish adding group** window, review the information and if anything needs to be changed, select the appropriate **Edit** option; otherwise, select the **Create group** button at the bottom of the page.
12. On the **New group created** window, note the message that appears at the top of the page that indicates it may take up to 5 minutes before the group appears in the list of active groups. Select **Close**
13. On the **Active groups** window, select **Refresh** on the menu bar to refresh the list of active groups. You may have to wait a few minutes and refresh again. Once the **Finance** group appears in the list, select the group.
14. For security purposes, you have decided to add Diego Siciliani as an additional owner of this group. In the **PND Group** pane that appears, the **General** tab is displayed by default. Select the **Members** tab.
15. In the **Members** tab, under the **Owners** group, select **View all and manage owners**.
16. In the **PND Group** group window, select **+Add owners**. This displays the list of current users, as well as the existing owner (the MOD Administrator).
17. In the Search field, enter **Diego**, select **Diego Siciliani**, and then select **Save**.
18. Select **Close**. This displays the list of owners for this group. Select **Close** again.
19. In the **Members** tab, under the **Members** group, select **View all and manage members**.
20. In the **PND Group** group window, select **+Add members**. This displays the list of current users.
21. In the list of users, it may be easier to enter the first few characters of each user's first name in the Search field rather than scrolling through the list of all on-premises users that were synchronized to Microsoft 365 in the earlier directory synchronization lab.

    Select **Isaiah Langer**, **Nestor Wilke**, and **Patti Fernandez** and then select **Save**.
22. Select **Close**. This displays the list of users for this group. Select **Close** again.
23. On the **PND Group** window, select the **X** in the upper right-hand corner to close the window.
24. Leave your Edge browser and all its tabs open and proceed to the next task.

47.0.2 Task 2 - Creating Sensitivity Labels using the Security and Compliance Center

Holly has decided to test creating sensitivity labels using both the Microsoft 365 Security and Compliance Center and Windows PowerShell. In this task you will use the Security and Compliance Center for this portion of your test.

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. In your Edge browser, you should still have a tab open for the **Microsoft Office Home** page and the **Microsoft 365 admin center** and you should still be logged in as Holly Dickson.

    Select the **Microsoft 365 admin center** tab.
3. In the **Microsoft 365 admin center**, select **Show all** in the left navigation pane and then under **Admin centers**, select **Security**.

4. In the **Office 365 Security and Compliance** center, in the left-hand navigation pane, select **Classification**, and then select **Sensitivity labels**.
5. On the **Sensitivity** page, the **Labels** tab is displayed by default. On the menu bar above the list of labels, select **Create a label**. This initiates a wizard to create a new sensitivity label.
6. In the **New sensitivity label** wizard, on the **Name and create a tooltip for your label** page, enter **Classified** in the **Name** field, and enter **For Official Use Only** in the **Description for Users** field. Select **Next**.
7. On the **Encryption** page, select the drop-down arrow in the **Encryption** field and then select **Apply**. This displays a number of encryption options.
8. In the **Assign Permissions now or let users decide?** field, select **Let users assign permissions when they apply the label**.
9. Select the **In Outlook, enforce restrictions equivalent to the Do Not Forward Option** check box.
10. Select **Next**.
11. On the **Content marking** page, select the toggle switch to turn **ON** Content Marking. This displays several additional options, which should be update in the following steps.
12. Select the **Add a watermark** check box and then select **Customize text**.
13. In the **Customize watermark text** window, enter the following information and then select **Save**:
    - Watermark text: **CLASSIFIED**
    - Font size: **48**
    - Font color: **RED**
    - Text layout: **Diagonal**
14. Select the **Add a header** check box and then select **Customize text**.
15. In the **Customize header text** window, enter the following information and then select **Save**:
    - Header text: **FOR OFFICIAL USE ONLY**
    - Font size: **12**
    - Font color: **Blue**
    - Align text: **Left**
16. Select the **Add a footer** check box and then select **Customize text**.
17. In the **Customize footer text** window, enter the following information and then select **Save**:
    - Footer text: **CONFIDENTIAL**
    - Font size: **12**
    - Font color: **Green**
    - Align text: **Left**
18. On the **Content marking** page, select **Next**.
19. On the **Auto-labeling for Office apps** page, verify the switch is turned **OFF** (it should be by default; if not, select **OFF**) and then select **Next**.
20. On the **Review your settings** page, review the entries that you made. If any need to be corrected, select the corresponding **Edit** option and make the necessary changes. When all settings are correct, select **Create label**.
21. On the **Your label was created** page, select **Done**.
22. Leave your Edge browser and all its tabs open and proceed to the next task.

47.0.3 Task 3 - Creating Sensitivity Labels using Windows PowerShell

Holly has decided to test creating sensitivity labels using both the Security and Compliance Center and Windows PowerShell. In this task you will use Windows PowerShell for this portion of your test.

Note: What Holly will learn from this task is that due to a current limitation, only the basic parameters for a sensitivity label can be updated in PowerShell at this time. The remaining parameters will have to be entered using the Security and Compliance Center.

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. Select the **magnifying glass (Search)** icon in the bottom left corner of your taskbar and then enter **powershell** in the Search field.
3. In the list of search results, right-click on **Windows PowerShell**, and in the menu that appears select **Run as administrator**.
4. Maximize your PowerShell window. In **Windows PowerShell**, at the command prompt type the following command and then press Enter:

   ```
   Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
   ```

   You will be prompted to confirm whether you want to change the execution policy. Enter **A** for **[A] Yes to all**.
5. At the command prompt enter the following command and then press Enter:

   ```
   Import-Module ExchangeOnlineManagement
   ```
6. At the command prompt enter the following command and then press Enter (remember to replace ZZZZZZ with the tenant ID provided by your lab hosting provider:

   ```
   Connect-IPPSSession -UserPrincipalName Admin@M365xZZZZZZ.onmicrosoft.com
   ```

   You will then be prompted to enter the Password for the MOD Administrator account. Enter the tenant admin password and then seelct **Sign in**.
7. At the command prompt enter the following command and then press Enter to validate that your are connected to the Microsoft 365 Compliance center:

   ```
   Get-DlpSensitiveInformationType -Identity "Credit Card Number"
   ```
8. At the command prompt enter the following command and then press Enter to create a new sensitivity label named "Secret", set its Tooltip to "Use it for Government Contracts ONLY" and changes the text color to Red:

   ```
   New-Label -DisplayName Secret -Tooltip "For use with Government contracts ONLY" -AdvancedSettings
   ```

   While the command updated the Display Name, you will be prompted to enter the label's Name. At the **Name** prompt, enter **Secret** and then press Enter.

   The policy will be displayed and it will be enabled (Disabled = False).
9. At the command prompt enter the following command and then press Enter to apply a Description to the Secret label (**Note:** At this time, this is the only label parameter you can set in PowerShell without extensive Scripts from JSON):

   ```
   Set-Label -Identity Secret -Comment "For use with Government contracts ONLY"
   ```
10. On the taskbar, select the Edge browser icon, and then select the **Security and Compliance** tab. You should still be in the **sensitivity** page and it should be displaying the **Labels** tab for this page.
11. In the list of labels, the **Classified** label that you created earlier should be displayed. Select **Refresh** on the menu bar above the list of labels.
12. In the list of labels, you should now see the **Classified** label that you created using the Security and Compliance Center and the **Secret** label that you created using Windows PowerShell.

    Select the **Secret** label.
13. In the **Secret** pane that appears, note that only the Name, Display Name, and Description were provided at the time the label was created in PowerShell. As mentioned earlier, this is due to a current limitation where these are the only parameters that can be entered for a sensitivity label in PowerShell at this time.

    To enter the remaining parameters for this Secret label, select **Edit label**.
14. On the **Name and create a tooltip for your label** page, select **Next**.
15. On the **Encryption** page, select the drop-down arrow in the **Encryption** field and then select **Apply**. This displays a number of encryption options.
16. In the **Assign Permissions now or let users decide?** field, select **Let users assign permissions when they apply the label**.

17. Select the **In Outlook, enforce restrictions equivalent to the Do Not Forward Option** check box.
18. Select **Next**.
19. On the **Content marking** page, select the toggle switch to turn **ON** Content Marking. This displays several additional options, which should be update in the following steps.
20. Select the **Add a watermark** check box and then select **Customize text**.
21. In the **Customize watermark text** window, enter the following information and then select **Save**:
    - Watermark text: **CLASSIFIED**
    - Font size: **48**
    - Font color: **RED**
    - Text layout: **Diagonal**
22. Select the **Add a header** check box and then select **Customize text**.
23. In the **Customize header text** window, enter the following information and then select **Save**:
    - Header text: **TOP SECRET**
    - Font size: **12**
    - Font color: **Blue**
    - Align text: **Left**
24. Select the **Add a footer** check box and then select **Customize text**.
25. In the **Customize footer text** window, enter the following information and then select **Save**:
    - Footer text: **CONFIDENTIAL**
    - Font size: **12**
    - Font color: **Green**
    - Align text: **Left**
26. On the **Content marking** page, select **Next**.
27. On the **Auto-labeling for Office apps** page, verify the switch is turned **OFF** (it should be by default; if not, select **OFF**) and then select **Next**.
28. On the **Review your settings** page, review the entries that you made. If any need to be corrected, select the corresponding **Edit** option and make the necessary changes. When all settings are correct, select **Save label**.
29. On the **Label updated** page, select **Done**.
30. Leave your Edge browser and all its tabs open and proceed to the next task.

47.0.4 Task 4 - Creating Sensitivity Label Policies using the Security and Compliance Center

Holly has decided to test creating sensitivity label policies using both the Microsoft 365 Security and Compliance Center and Windows PowerShell. In this task you will use the Security and Compliance Center for this portion of your test.

1. On **LON-CL1** you should still be in the **Security and Compliance** tab, which should be displaying the **sensitivity** page. You are currently displaying the **Labels** tab for this page.

   In the list of tabs across the top of the page, select **Label policies**.
2. On the **Label policies** page, on the menu bar above the list of policies, select **Publish labels**. This initiates a wizard to create a new sensitivity label policies.
3. In the **Create policy** wizard, on the **Choose sensitivity labels to publish** page, select **Choose sensitivity labels to publish**.
4. On the **Sensitivity labels to publish** pane that appears, select **Classified** and then select **Add** (Note - you will publish the Secret label in the next task using Windows PowerShell).
5. On the **Choose sensitivity labels to publish** page, select **Next**.
6. On the **Publish to users and groups** page, you will define the users and groups to which this published label will be made available. Note that the **Users and groups** is set by default to **All**, which will include all users and groups in the organization. Select **Next**.

7. On the **Policy Settings** page, leave the current selection of **None** and select **Next**.
8. On the **Name your policy** page, enter **Classified Policy** in the **Name** field and enter **This policy is used for sensitive information in Government contracts only**. Select **Next**.
9. On the **Review and finish** page, review the entries that you made. If any need to be corrected, select the corresponding **Edit** option and make the necessary changes. When all settings are correct, select **Submit**.
10. On the **New policy created** page, select **Done**.
11. Leave your Edge browser and all its tabs open and proceed to the next task.

47.0.5 Task 5 - Creating Sensitivity Label Policies using Windows PowerShell

Holly has decided to test creating sensitivity label policies using both the Security and Compliance Center and Windows PowerShell. In this task you will use Windows PowerShell for this portion of your test.

Note: What Holly will learn from this task is that due to a current limitation, only the basic parameters for a sensitivity label can be updated in PowerShell at this time. The remaining parameters will have to be entered using the Security and Compliance Center.

1. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.
2. Windows PowerShell should still be open from a prior task. If so, then skip to the next step. However, if you closed PowerShell, then open an elevated instance of it now (Run as administrator) and run the following commands to re-establish your session:

   ```
   Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
   ```

   You will be prompted to confirm whether you want to change the execution policy. Enter **A** for [**A**] **Yes to all**.

   ```
   Import-Module ExchangeOnlineManagement

   Connect-IPPSSession -UserPrincipalName Admin@M365xZZZZZZ.onmicrosoft.com

   (remember to replace ZZZZZZ with the tenant ID provided by your lab hosting provider)
   ```

   You will then be prompted to enter the Password for the MOD Administrator account. Enter the tenant admin password and then seelct **Sign in**.
3. At the command prompt enter the following command and then press Enter to create a new Sensitivity label policy named “Secret” using the secret Label that you created in the earlier task. This label policy will be applied to the PND Group group and will use the highest-level label as the default for documents and will automatically apply the label to emails and documents sent from this group. Do not forge to replace ZZZZZZ with the tenant ID provided by the lab hosting provider.

   ```
   New-LabelPolicy -Name "Secret policy" -Labels "Secret" -Comment "This policy is for the Microsoft
   ```
4. At the command prompt enter the following command and then press Enter:

   ```
   Set-LabelPolicy -Identity "Secret policy" -AdvancedSettings @{DisableMandatoryInOutlook="True"}
   ```
5. On the taskbar, select the Edge browser icon, and then select the **Security and Compliance** tab. You should still be in the **sensitivity** page and it should be displaying the **Label policies** tab for this page.

   In the list of label policies, the **Classified** label that you created earlier should be displayed. Select **Refresh** on the menu bar above the list of labels.
6. In the list of label policies, you should now see the **Classified policy** that you created using the Security and Compliance Center and the **Secret policy** that you created using Windows PowerShell.
7. Close Windows PowerShell.
8. Leave your Edge browser and all its tabs open and proceed to the next lab.

48 End of Lab 11

49 Module 12 - Lab 12 - Exercise 1 - Monitoring Microsoft 365 Service Health

As Holly Dickson concludes her Microsoft 365 pilot project, she is interested in viewing the health of Adatum's Microsoft services, including Office on the web, Yammer, and mobile device management cloud services. After doing a little research, Holly has discovered that this information is available on the Service health page in the Microsoft 365 admin center. Therefore, if Adataum experiences problems with a cloud service, Holly can check its service health to determine whether this is a known issue with a resolution in progress before she calls Microsoft Support or spends time troubleshooting.

In this exercise, Holly will view the Microsoft 365 service health and several service health reports in the Microsoft 365 admin center.

49.0.1 Task 1- View Microsoft 365 service health

1. On **LON-CL1** you should still be logged in as the **Administrator** from the prior lab exercise.
2. In your Edge browser, you should still have a tab open for the **Microsoft Office Home** page and the **Microsoft 365 admin center** and you should still be logged in as Holly Dickson.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all**, select **Health**, and then select **Service health**.
4. On the **Service health** page, in the list of services, the **Exchange Online** service displays 1 incident in the **Status** column. Select this **1 incident**.
5. This displays the **Incidents** tab on the **Service health** page. In the list of incidents, it only displays this one incident related to Exchange Online. Select the title for this incident. This opens an information pane on the right side of the screen that provides details on this incident. Review this information, then close this incident pane.
6. On the **Service health** page, select **All services** on the menu bar.
7. On the **Service health** page, in the list of services, the **Microsoft 365 suite** service displays 2 advisories in the **Status** column. Select this **2 advisories**.
8. This displays the **Advisories** tab on the **Service health** page. In the list of advisories, it only displays these two advisories related to Microsoft 365. Select the title for the first advisory. This opens an information pane on the right side of the screen that provides details on this advisory. Review this information, then close this incident pane. Repeat this for the second advisory.
9. On the **Service health** page, select **History** on the menu bar. This displays a history of incidents and advisories that have been resolved.
10. In the **Microsoft 365 admin center**, in the left-hand navigation pane under **Health**, select **Message center**.
11. The **Message Center** page displays a list of all active messages related to planned changes. Select a message to open a detail pane that provides a high-level overview of the planed change. Review any of the messages that interest you.
12. Select any entry in the list to view the details about it. Close the detail pane to return to the history list. Repeat this for any event that interests you.
13. Leave the Edge browser and all its tabs open and proceed to the next task.

49.0.2 Task 2 - View reports in the Microsoft 365 admin center

1. On **LON-CL1** you should still be logged in as the **Administrator** from the prior lab exercise. In your Edge browser, you should also be logged into Microsoft 365 as Holly Dickson.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Reports**. Note that as of this writing there are only 3 reports listed in this group. Select each of the reports to view information related to it.

3. Microsoft 365 includes a variety of additional reports, which can be found in the portals to which they apply. For example:
    - **Security reports** are included in the Reports dashboard in the Security and Compliance Center. In the **Microsoft 365 admin center**, under the **Admin centers** group, select **Security**. This opens the **Security and Compliance Center**. In the navigation pane under **Reports**, select **Dashbaoard**.
    - **Auditing reports** are included in the Exchange admin center. In the **Microsoft 365 admin center**, under the **Admin centers** group, select **Exchange**. This opens the **Exchange admin center**. In the navigation pane select **Compliance management**, and then on the **Compliance management** page, select the **auditing** tab.

    Review any of the reports that are of interest to you.

    Note: Most of the reports have limited data due to the lack of data in your virtualized lab environment for the fictitious Adatum Corporation.
4. Leave the Edge browser open, and leave the **Microsoft Office Home** tab open as well as the **Microsoft 365 admin center** tab. However, close all other tabs and then proceed to the next task.

Results: After completing this exercise, you should have monitored the health of Microsoft 365 services and viewed reports in the Microsoft 365 admin center.

50 Proceed to Lab 12 - Exercise 2

51 Module 12 - Lab 12 - Exercise 2 - Troubleshooting Mail Flow Issues

The logical conclusion to monitoring Microsoft 365 service health is the ability to troubleshoot errors that occur in the system. For Holly Dickson, this means monitoring mail-related issues, which have been a nagging issue for Adatum in the past. Holly plans to take advantage of Microsoft's Exchange Remote Connectivity Analyzer tool to troubleshoot mail-flow issues. The tool is web-based and is designed to help IT Administrators troubleshoot connectivity issues that affect their Microsoft Exchange deployments. The tool simulates several client log-on and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist the IT Administrator to correct the problem.

Holly plans to test this tool by sending email to a non-existent domain and to a non-existent user and then use the tool to troubleshoot the errors that occur. She will then test message tracing to help troubleshoot mail-flow issues. Message tracing in the Security and Compliance Center follows email messages as they travel through an Exchange Online organization. Holly will use message tracing to determine if a message was received, rejected, deferred, or delivered by the service. She will also use it to show what actions were taken on the message before it reached its final status.

51.0.1 Task 1 - Send an email to a non-existent domain

1. On **LON-CL1** you should still be logged in as the **Administrator** from the prior lab exercise.
2. Your Edge browser should still be open, and you should be logged into Microsoft 365 as Holly Dickson. You should have tabs open for the **Microsoft Office Home** page and the **Microsoft 365 admin center**.
3. Select the **Microsoft Office Home** tab, and in the Office portal, select **Outlook**.
4. In **Outlook on the web**, select **New message**.
5. In the message form, type **user@alt.none** in the **To** box.
6. Enter a subject and some body text and then select **Send**.
7. Wait for the delivery failure message to appear.
8. Once the delivery failure message arrives, select the delivery failure message. Note the reason for the failure: **The Domain Name System (DNS) reported that the recipient's domain does not exist.**
9. Scroll down in the text portion of the message to the **Diagnostic information for administrators** section. Select all the text in this section (starting with **Generating server** down to the end of this diagnostic data), and then press **Ctrl+C** to copy it to the clipboard.

10. In Microsoft Edge, open a new tab and enter the following URL in the address bar: **https://testconnectivity.microso**
11. This opens the **Microsoft Remote Connectivity Analyzer** page. In the left-hand navigation pane, select the **Message Analyzer** tab.
12. In the **Message Header Analyzer** page, in the section that displays **Paste headers here**, press **Ctrl-V** to paste in the header data that you copied to the clipboard, and then select **Analyze headers**.
13. Review the diagnostic information and the time taken for the message to be rejected.
14. Select **Clear** to reset the Message Header Analyzer.
15. Leave the Edge browser and all tabs open and proceed to the next task.

51.0.2 Task 2 - Send an email to a non-existent user

1. In the **Edge** browser, select the **Outlook** tab for Holly Dickson.
2. In **Outlook on the web**, select **New message**.
3. In the message form, type **ynotknirf082760@outlook.com** in the **To** box.
4. Enter a subject and some body text and then select **Send**.
5. Wait for the delivery failure message to appear.
6. Once the delivery failure message arrives, select the delivery failure message. Note the reason for the failure: **Requested action not taken: mailbox unavailable**
7. Scroll down in the text portion of the message to the **Diagnostic information for administrators** section. Select all the text in this section (starting with **Generating server** down to the end of this diagnostic data), and then press **Ctrl+C** to copy it to the clipboard.
8. In Microsoft Edge, select the **Message Analyzer** tab.
9. In the **Message Header Analyzer** page, in the section that displays **Paste headers here**, press **Ctrl-V** to paste in the header data that you copied to the clipboard, and then select **Analyze headers**.
10. Review the diagnostic information and the time taken for the message to be rejected.
11. Select **Clear** to reset the Message Header Analyzer.
12. In the **Edge** browser, close all tabs except for the **Microsoft Office Home** tab.

51.0.3 Task 3 - Analyze mail flow

In this task, you will conduct a message trace to monitor message flow. Note that the original Message Trace feature was provided through the Exchange Online admin center. However, a new and improved Message Trace feature has been added to the Security and Compliance Center, which is the message trace feature that will be used in this lab.

1. In the **Edge** browser on **LON-CL1**, the **Microsoft Office Home** tab should still be open from the prior task. In this tab, select **Admin**.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all**, and then under **Admin centers** select **Security**.
3. In the **Office 365 Security and Compliance** center, in the left-hand navigation pane, select **Mail flow** and then select **Message trace**.
4. In **Message trace** page, note the existing queries that you can use. However, in this case, you will create a custom message trace. Select **+Start a trace**.
5. In the **New message trace** window, select the **By these people** field. In the list of users that appears, select **Holly Dickson**.
6. In the **Within this time range** chart, move the slider to **1 day** (this will show the past 24 hours).
7. Select **More search options**, and then in the **Delivery status** field, select **Failed**.
8. Select **Search**.

9. On the **Message trace search results** page, note the two messages that appear. Double-click the message for the non-existent user. This opens the **Message trace details** pane, which displays the detailed information for the message, including the sender, recipient, message size, ID, and IP address information.

   Select the **Message events** and **More information** sections to expand them. As you review the information, pay special note to the following data: Receive, Submit, Span. Diagnostics, and Faild. Close the pane when you are finished.

10. Repeat the prior step for the non-existent domain message.

11. Close the Message Trace window.

52 End of Lab 12