Contents

1 MS-100T00: Microsoft 365 Identity and Services

- **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-100T00-Microsoft-365-Identity-and-Services/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

2.3 {% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MS-100T00-Microsoft-365-Identity-and-Services/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

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

3 Demo: Deploying an ARM Template

3.1 Instructions

1. Quisque dictum convallis metus, vitae vestibulum turpis dapibus non.

    1. Suspendisse commodo tempor convallis.

    2. Nunc eget quam facilisis, imperdiet felis ut, blandit nibh.

    3. Phasellus pulvinar ornare sem, ut imperdiet justo volutpat et.

2. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

3. Vestibulum hendrerit orci urna, non aliquet eros eleifend vitae.

4. Curabitur nibh dui, vestibulum cursus neque commodo, aliquet accumsan risus.

    `Sed at malesuada orci, eu volutpat ex`

5. In ac odio vulputate, faucibus lorem at, sagittis felis.

6. Fusce tincidunt sapien nec dolor congue facilisis lacinia quis urna.

    Note: Ut feugiat est id ultrices gravida.

7. Phasellus urna lacus, luctus at suscipit vitae, maximus ac nisl.

    - Morbi in tortor finibus, tempus dolor a, cursus lorem.

    - Maecenas id risus pharetra, viverra elit quis, lacinia odio.

    - Etiam rutrum pretium enim.

8. Curabitur in pretium urna, nec ullamcorper diam.

4 Module 2 - Lab 1 - Exercise 1 - Initialize your Microsoft 365 Tenant

Adatum Corporation runs their legacy applications (such as Microsoft Exchange Server 2019) 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.

As Adatum's Enterprise administrator, you have been tasked with deploying Microsoft 365 in Adatum's hybrid deployment using a virtualized lab environment. In this exercise, you will set up Adatum's Microsoft 365 trial tenant, and your instructor will guide you 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 created a free Microsoft 365 trial tenant for you, along with a default tenant admin account in Microsoft 365 (the display name for this user account is MOD Administrator). You will log into the Domain Controller VM (LON-DC1) using the local ADATUM\Administrator account, and when you access Microsoft 365 for the first time, you will initially log in using the Microsoft 365 tenant admin account created by your lab hosting provider. You will then update Adatum's Microsoft 365

organizational profile, and you will prepare your tenant for Microsoft Azure Active Directory and for a future lab using Microsoft Teams.

4.0.1 Task 1 - Obtain Your Microsoft 365 Credentials

Once you launch the lab, a free trial tenant will be automatically created for you to access Microsoft 365 in the Microsoft Virtual Lab environment. Within this tenant, your lab hosting provider will create a Microsoft 365 user account for a default tenant administrator named MOD Administrator. Your lab hosting provider will assign this user account a unique username and password, and the account will be assigned the Microsoft 365 Global administrator role. You must retrieve this username and password so that you can sign into Microsoft 365 within the Microsoft Virtual Lab environment under the resource section. You will also be assigned a unique network IP address and UPN name for your Microsoft 365 blob. You will also use this UPN name in various tasks throughout the labs for this course.

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 prefix.** This tenant prefix is for the Microsoft 365 user accounts that you will use to sign into Microsoft 365 throughout the labs in this course. The domain for each Microsoft 365 user account is in the format of {user alias}@xxxxxZZZZZZ.onmicrosoft.com, where xxxxxZZZZZZ is the tenant prefix. It consists of two parts - your lab hoster's prefix (xxxxx; some hosters use a generic prefix such as M365x, while others use their company initials or some other designation) and the tenant ID (ZZZZZZ; usually a 6 digit number). Record this xxxxxZZZZZZ tenant prefix value for later use. When any of the lab steps direct you to sign into Microsoft 365 as one of the user accounts (such as the MOD Administrator), you must enter the xxxxxZZZZZZ value that you obtained here as the tenant prefix portion of your .onmicrosoft.com domain.

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

- **Custom Domain name.** Your lab hosting provider has created a custom domain name for Adatum that you will use when adding a custom domain into Microsoft 365 in a later lab exercise. The domain name is in the format **xxxUPNxxx.xxxCustomDomainxxx.xxx.** You must replace **xxxUPNxxx** with the UPN name provided by your lab hosting provider, and you must replace **xxxCustomDomainxxx.xxx** with the lab hosting provider's domain name. For example, let's assume your lab hosting provider is Fabrikam Inc. If the UPN number it assigns to your tenant is AMPVU3a and its custom domain name is fabrikam.us, then the domain name for your new custom domain would be AMPVU3a.fabrikam.us. Your instructor will provide you with your lab hosting provider's UPN number and custom domain name.

- **Network IP address.** Write down the **IP Address** value (this is the IP Address of your parent domain; for example, 64.64.206.13).

4.0.2 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 the next lab exercise), Holly will initially sign into Microsoft 365 using the default Microsoft 365 tenant admin account and password that was created by your lab hosting provider. This account will be admin@xxxxxZZZZZZ.onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix assigned by your lab hosting provider); the display name for this account will be MOD Administrator.

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 machines, either the local client PC (LON-CL1) or Adatum's on-premises Exchange Server (LON-EX1), then switch to LON-DC1 now.

2. On **LON-DC1**, you must select **Ctrl+Alt+Delete** to log in (your instructor will guide you on how to find this option in your VM environment). Log into LON-DC1 as the **Administrator** with the password **Pa55w.rd**.

3. If you receive a **Windows License** warning message asking you to activate Windows in Settings. Select **Close**. If you also 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 (it's used in the next task) but minimize the window for now.

5. On the taskbar at the bottom of the page, select the **Internet Explorer** icon. If necessary, 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 the **Tenant Username** provided by your lab hosting provider (**admin@xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is the tenant prefix assigned by your lab hosting provider) and then select **Next**.

8. In the **Enter password** dialog box, copy and paste in the unique **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. On the **Microsoft Office Home** tab, notice the initials **MA** that appear in a circle in the top-right corner of the screen. These are the initials of the **MOD Administrator** account, which is the tenant admin account created by your lab hosting provider that you just signed in as. The other existing Microsoft 365 user accounts that were created by your lab hosting provider have a picture associated with each of their accounts; therefore, in later labs when you sign in as any of these users, the user's picture will be displayed rather than the user's initials. However, when a user such as the MOD Administrator has no picture assigned to it, the user's initials are displayed in place of the picture.

    On the **Microsoft Office Home** tab, in the column of Microsoft 365 app icons that appears on the left side of the screen, select the **Admin** icon, which is the last icon in the list; this opens the **Microsoft 365 admin center** in a new browser tab.

12. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all** and then select **Settings**. In the **Settings** group, select **Org settings**.

13. On the **Org settings** page, the **Services** tab at the top of the page is displayed by default. To the right of the **Services** tab is the **Organization profile** tab; select this tab now.

14. On the **Org settings** page, in the **Organization profile** tab, select **Organization information** from the list of profile data.

15. In the **Organization information** pane that appears, enter the following information:

    - Name: **Adatum Corporation** (Note: Contoso is originally displayed as the organization name; this was explained in the Introduction section at the start of this lab. In this step you will change it to Adatum Corporation.)
    - Street Address: **555 Main Street**
    - City: **Redmond**
    - State or province: **Washington**
    - ZIP or postal code: **98052**
    - Phone: do not change
    - Technical contact: do not change
    - Preferred language: **English**

16. Select **Save**.

17. At the top of the **Organization information** pane, note the message indicating the changes have been saved. Select the **X** in the upper right-hand corner to close the pane.

18. Back on the **Organization profile** tab, in the list of organization profile data, select **Release preferences**.

19. In the **Release preferences** pane that appears, select the **Targeted release for select users** option and then select **Save**.

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

    Note: This **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 a select group of users is the more typical preference as it enables an organization to control when it wants to make updates available to everyone once they've been reviewed by the control group.

20. In the **Release preferences** pane, below the list of release options, select **Select users**.

21. In the **Choose users for targeted release** pane that appears, select inside the **Who should receive targeted releases?** field. This displays the list of active users (these are the ten Microsoft 365 user accounts created for your tenant by your lab hosting provider). In this list, select each of the following users (Note: You have to select each user, one at a time; after selecting a user, you must select inside the field again to re-display the list so that you can display the next user):

    - **Alex Wilber**
    - **Joni Sherman**
    - **Lynne Robbins**
    - **MOD Administrator**

    Note: Alex, Joni, and Lynne are administrators who are part of Holly's pilot team. Their accounts will be used throughout the labs for this course.

22. Select **Save**.

23. Verify the users you selected appear at the bottom of the **Release preferences** pane, and then select the **X** in the upper-right corner of the **Release preferences** pane to close it.

24. In the list of organization profile data, select **Custom themes**.

25. In the **Custom themes** pane, scroll to the bottom of the pane and select the **Show the user's display name** check box.

    As you scroll through the pane, review the various theme and branding options that are available for you to update. For 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.

    Tip: 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. Select **Save** when you are done and then close the **Custom themes** pane once your changes have been saved.

4.0.3 Task 3 – Prepare for Microsoft Azure Active Directory

Azure Active Directory is needed to perform several configuration steps when installing Microsoft 365. To access Azure Active Directory, you must first prepare for it by performing the following tasks: installing the Microsoft Online Services Sign-In Assistant and installing the Windows Azure Active Directory PowerShell Module.

- **Install the Microsoft Online Services Sign-In Assistant.** The Microsoft Online Services Sign-In Assistant (MOS SIA) provides end-user sign-in capabilities to Microsoft Online Services, such as Microsoft 365. The MOS SIA installs client components that allow applications, such as Microsoft Outlook and the Windows Azure Active Directory PowerShell Module, to authenticate to Microsoft Online Services. The MOS SIA can also provide an improved sign-in experience, where end-users can access Microsoft Online Services without having to re-enter their credentials.

- **Install the Windows Azure Active Directory PowerShell Module.** To manage users and organization settings in Microsoft 365 through Windows PowerShell, you must first install the Azure Active Directory PowerShell Module. This can simply be installed through PowerShell itself. This module allows you to perform many of the Microsoft 365 user and organization administration tasks through PowerShell. It's great for bulk tasks such as password resets, password policies, license management and reporting, and so on.

1. On LON-DC1, you must navigate to the **Microsoft Download Center** to download the **Microsoft Online Services Sign-In Assistant for IT Professionals RTW** wizard.

   To do so, open a new tab in your **Edge** browser session and then enter the following URL in the address bar: **https://aka.ms/AA6zxrs**

2. On the **Microsoft Download Center** page, scroll down to the **Microsoft Online Services Sign-In Assistant for IT Professionals RTW** section, leave **English** as the selected language and then select the **Download** button.

3. In the **Choose the download you want** window, select the **msoidcli_64bit.msi** check box and then select **Next**.

4. In the notification bar at the bottom of the page that displays the download status of the msoidcli_64bit.msi file, select **Open file** once the download is complete.

5. If a **Do you want to allow pop-ups?** dialog box appears, select **Allow Once** or **Always allow on theis site**. If a **Do you want to run this file?** dialog box appears, select **Run**.

6. 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**.

7. Once the installation is complete, on the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, select **Finish**.

8. Close the **Download Microsoft Online Services** tab in your Edge browser.

9. 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 list of search results, right-click on **Windows PowerShell** (do not select Windows PowerShell ISE) and select **Run as administrator** in the drop-down menu that appears or while highlightening **PowerShell .

10. Maximize your PowerShell window. In **Windows PowerShell**, at the command prompt type the following command and then press Enter:

    ```
    Install-Module MSOnline
    ```

11. If you are prompted to install the **NuGet provider,** enter **Y** to select **[Y] Yes**.

12. 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.**

13. Once the installation is complete, the screen will return to the Windows PowerShell command prompt. You must then run the following command to install the Azure AD PowerShell module that you just retrieved in the earlier step:

    ```
    Install-Module AzureADPreview
    ```

14. 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.**

15. 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.

16. Leave the Windows PowerShell window open but minimize it for now.

17. Remain logged into LON-DC1 and keep your Edge browser open.

4.0.4 Task 4 – Prepare for External Access using Microsoft Teams

When you get to Module 4, you will perform a lab in which you will create a new service request ticketing system. One of the tasks within that lab requires you to collaborate with one of your fellow student's Microsoft 365 tenant through Microsoft Teams. To enable this communication between your tenant and your fellow student's tenant, you must turn on the **External Access** functionality within Teams. When you turn on this External

Access feature, it can take a couple of hours for your system to propagate the changes through your tenant. Therefore, you will turn on this External Access feature in this task so that the internal changes made by the system have time to propagate through your tenant by the time you eventually get to the Module 4 lab.

Instructor/Student Note: To facilitate this lab, your instructor should collect each student's tenant ID (ZZZZZZ) from each of their domains (this would be each student's xxxxxZZZZZZ.onmicrosoft.com domain, where xxxxxZZZZZZ is the tenant prefix assigned by your lab hosting provider; ZZZZZZ is the tenant ID portion of the tenant prefix that is unique to each student). The instructor will then assign to each student the tenant ID (ZZZZZZ) from another student (you can NOT be assigned your own tenant ID). When you enable External Access in this task, you will enter the domain associated with the assigned tenant ID from your fellow student (in other words, you will enter the **xxxxxZZZZZZ.onmicrosoft.com** domain, where ZZZZZZ is your fellow student's tenant ID).

By the time you get to the Module 4 labs, External Access should be ready so that you can collaborate with the student whose domain you set up in this task. Conversely, you should also be able to collaborate with the student who entered your domain in his or her External Access setup.

1. On LON-DC1, in your Microsoft Edge browser, you should still be logged into the Microsoft 365 admin center as the MOD Administrator from the earlier task in which you updated Adatum's organizational profile.

   If you closed the Microsoft 365 admin center, then perform the same steps as before to open it and sign in as **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix assigned by your lab hosting provider) with the tenant admin password provided by your lab hosting provider.

2. If necessary, in the **Microsoft 365 admin center**, in the left-hand navigation pane, select **...Show All** to display all the navigation menu options.

3. In the **Microsoft 365 admin center**, in the left-hand navigation pane under the **Admin Centers** group, select **Teams**.

4. A new tab will open in your Edge browser that displays the **Microsoft Teams admin center**. If a **Welcome to the Teams admin center** window appears, select **Skip tour**.

5. In the **Microsoft Teams admin center**, in the left-hand navigation pane, select **Org-wide settings** and then select **External access**.

6. On the **External access** page, confirm that the toggle switches for both external access options are in the **On** position. If either are set to **Off**, then set them to **On** now.

7. Below the toggle switches, select **+Add a domain**.

8. In the **Add a domain** pane that appears, enter **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ **is your fellow student's tenant prefix** that was assigned to you by your instructor) in the **Domain** field. **Do NOT enter your own tenant prefix.**

9. In the **Action to take on this domain** field, select **Allowed**, and then select **Done**.

10. On the **External access** page, select **Save**.

11. In your Microsoft Edge browser, close the **External access - Microsoft Teams** tab. This should return you to the **Microsoft 365 admin center** tab, which you should leave open as you proceed to the next exercise.

5   Proceed to Lab 1 - Exercise 2

6   Module 2 - Lab 1 - Exercise 2 - Manage Users and Groups

In the following lab exercise, you will take on the role of Holly Dickson, Adatum Corporation's Enterprise Administrator. In this exercise, you will perform several user and group management functions within Microsoft 365. You will begin by creating a Microsoft 365 user account for Holly, who will be assigned the Global Admin role. You will create two Microsoft 365 groups and assign existing Microsoft 365 users as members of those groups. You will then delete one of the groups and then use Windows PowerShell to recover the deleted group.

Note: The VM environment provided by your lab hosting provider comes with ten existing Microsoft 365 user accounts, as well as a large number of existing on-premises user accounts. Several of the existing Microsoft 365 user accounts will be used throughout the labs in this course. This will save you from having to perform the

tedious task of creating user accounts, which is typically not a task performed by Enterprise Administrators. Even though the MOD Administrator account has been set up for you by your lab hosting provider, you will still create Holly Dickson's user account, since having more than one Global admin is a best practice. It will also provide you with the experience of creating a Microsoft 365 user account in case you are not familiar with the process.

6.0.1   Task 1 - Create a User Account for Adatum's Enterprise Administrator

Holly Dickson is Adatum's Enterprise Administrator. Since a Microsoft 365 user account has not been set up for her, she initially signed into Microsoft 365 as the MOD Administrator account (the default Global admin) in the previous lab (you did this when you began your role as Holly and signed in using the tenant admin account). In this task, you will continue in your role as Holly Dickson where you should still be logged into Microsoft 365 as the MOD Administrator. In this lab, Holly will create a personal 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. Following this task, you will perform all remaining labs using Holly's persona.

Important: As a best practice in your real-world deployment, you should always write down the first Global admin account's credentials (in this lab, the MOD Administrator account, whose username is admin@xxxxxZZZZZZ.onmicrosoft.com, where xxxxxZZZZZZ is the tenant prefix assigned by your lab hosting provider) and store it away for security reasons. **This account should be a non-personalized identity** that owns the highest privileges possible in a tenant. It should **not** be MFA activated (because it is not personalized). Because the username and password for this account are typically shared among several users, this first Global admin is a perfect target for attacks; therefore, it is always recommended that organizations create personalized service admin accounts and keep as few Global admins as possible. For those Global admins that you do create in your real-world deployment, they should each be mapped to a single identity (such as Holly Dickson), and they should each have Multi-Factor Authentication (MFA) enforced. That being said, you will not turn on MFA for Holly's account because time is limited in this training course and we do not want to take up lab time by making you log in using a second authentication method every time Holly logs in.

1. On LON-DC1, the **Microsoft 365 admin center** should still be open in your Edge browser from the prior lab, 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**.

3. In the **Active users** list, you will see the list of existing user accounts that were created for you by your lab hosting provider. In this task, you are taking on the role of the MOD Administrator, and as such, you must create a user account for Holly Dickson, who is Adatum's new Enterprise Administrator. In doing so, you will assign Holly the Microsoft 365 role of Global Administrator, which gives Holly global access to most management features and data across Microsoft online services.

4. In the **Active Users** window, select **Add user** that appears on the menu bar above the list of active users. In the drop-down menu that appears, select **Single user**. This initiates the **Add a user** wizard.

5. In the **Add a user** wizard, on the **Set up the basics** page, 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 should be prefilled with the **xxxxxZZZZZZ.onmicrosoft.com** cloud domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

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

     Holly@xxxxxZZZZZZ.onmicrosoft.com

   - Password settings: Clear (uncheck) the box next to **Automatically create a password**

   - Password: **Pa55w.rd** (Hint: Select the eye icon at the right side of the field to verify the password that you entered)

- Clear (uncheck) the **Require this user to change their password when they first sign in** check box

6. Select **Next**.

7. In the **Assign product licenses** page, enter the following information:

   - Select location: **United States**

   - Licenses: The **Assign user a product license** option should be selected by default; under this option, select **Office 365 E5**

8. Select **Next.**

9. In the **Optional settings** window, select the drop-down arrow to the right of **Roles.**

10. In the **Roles** section, select the **Admin center access** option. By doing so, the most commonly used Microsoft 365 administrator roles are enabled below this option.

    Note: If you scroll down past this list of the most commonly used admin roles and select **Show all by category**, the complete list of admin roles will be displayed (sorted by category). For Holly, you do not need to view all the admin roles by category, since Holly will be assigned the Global admin role that appears in the list of most commonly used roles.

11. Select the **Global admin** check box and then select **Next**.

12. 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**.

13. On the **Holly Dickson added to Active users** page, under the **User details** section, select **Show** next to the password to verify Holly's password is **Pa55w.rd** and then select **Close.**

    Note: If you accidentally entered a different password, then once you return to the **Active users** page, you must select the **Reset a password** icon (the key icon that appears when you hover over Holly's account) to change her password to **Pa55w.rd**.

14. If a survey window appears, select **Cancel**.

15. Remain logged into LON-DC1 with the **Microsoft 365 admin center** open in your browser for the next task.

6.0.2 Task 2 – Create and Manage Groups

After completing the previous task, you should still be signed into the **Microsoft 365 admin center** as the **MOD Administrator** account. In this task, you will begin implementing Adatum's Microsoft 365 pilot project as Holly Dickson, Adatum's new Enterprise Administrator. Therefore, you will begin this task by logging out of Microsoft 365 as the MOD Administrator and you will log back in as Holly.

In this task, you will create two new groups and then manage the groups by assigning users to them. One group will be a Microsoft 365 group and the other a Security group; this will enable you to see some of the differences in the two types of groups. After creating the groups, you will then delete one of them. This will set up the next task, which examines how to recover a deleted group using Windows PowerShell.

1. On LON-DC1, on the **Microsoft 365 admin center** tab in your Edge browser, select the user icon for the **MOD Administrator** (the **MA** circle) in the upper right-hand corner of your browser, and in the **MOD Administrator** window that appears, select **Sign out.**

   Important: When signing out of one user account and signing in as another, you should close all the browser tabs except for your current tab (which will be the **Sign out** tab). This is a best practice that helps to avoid any confusion by closing the windows associated with the prior user. Take a moment now and close all other browser tabs except for the **Sign out** tab.

2. In your Microsoft Edge browser, in the **Sign out** tab, enter the following URL in the address bar to sign back into Microsoft 365: **https://portal.office.com**

3. In the **Pick an account** window, only the tenant admin account (the admin@xxxxxZZZZZZ.onmicrosoft.com account) that you just logged out from appears. Select **Use another account**.

4. In the **Sign in** window, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). Select **Next**.

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

6. If a **Get your work done with Office 365** window appears, select the **X** to close it.

7. On the **Office 365 Home** page, in the column of Microsoft 365 app icons that appears along the left side of the screen, select the **Admin** icon to open the Microsoft 365 admin center in a new browser tab.

8. If a survey window appears, select **Cancel**.

9. In the **Microsoft 365 admin center**, select **Groups** in the left-hand navigation pane, and then under it, select **Active Groups**.

10. In the **Active groups** page, select **Add a group** that appears on the menu bar above the list of groups. This initiates the **Add a group** wizard.

11. In the **Add a group** wizard, on the **Choose a group type** page, select **Microsoft 365 (recommended)** and then select **Next**.

12. In the **Set up the basics** page, enter **Inside Sales** in the **Name** field, and then enter **Collaboration group for the Inside Sales team** in the **Description** field (even if you don't enter a description, you must still select into this field to enable the **Next** button). Select **Next**.

13. In the **Assign Owners** window, you will assign Allan Deyoung and Patti Fernandez as owners of this group.

    Select into the **Owners** field and in the list of users that appears, select **Allan Deyoung**.

    Select into the **Owners** field and in the list of users that appears, select **Patti Fernandez**.

    Select **Next**.

14. In the **Edit settings** page, enter the following information and then select **Next**:

    - Enter **insidesales** in the **Group email address** field
    - Under the **Privacy** section, select the **Public - Anyone can see group content** option (you must select it even if it's already selected in order to enable the **Next** button at the bottom of the page)
    - Under the **Add Microsoft Teams to your group** section, verify the **Create a team for this group** check box is selected (select it if need be)

15. In the **Review and finish adding group** page, review the content that you entered. If everything is correct, select **Create group**; otherwise, select **Back** and fix anything that must be corrected (or select **Edit** under the specific area that needs adjustment).

16. On the **New group created** window, note the comment at the top of the page that it may take 5 minutes for the new group to appear in the list of groups.

    Select **Close**. This returns you to the **Active groups** page.

17. Repeat steps 10-16 to add a new group with the following information:

    - Group type: **Security**
    - Name: **IT Admins**
    - Description: **IT administrative personnel**

    Note: there is no owner, email address, or privacy setting for Security groups

18. If either of the two new groups do not appear in the **Active groups** list, wait a minute or so and then select the **Refresh** option on the menu bar (to the right of **Add a group**). You may need to wait an additional minute or two for both groups to appear.

    Note: The IT admins group does not have a group email address because it's a Security group. Two additional group types are Mail-enabled Security groups and Distribution groups. Neither of these group types were used in this lab because it can take up to an hour for these two types of groups to appear in the Groups list; whereas Microsoft 365 groups and Security groups usually take just a matter of minutes to appear.

19. You're now ready to add members to the groups. In the list of **Active groups**, select the **Inside Sales** group.

20. In the **Inside Sales** pane that appears, the **General** tab is displayed by default. Select the **Members** tab.

21. The **Members** tab displays sections for the Owners and the Members. Under the **Owners** section, you can see the two owners (Allan and Patti). Under the **Members** section, you can see that there are zero (0) members. Under this section, select **View all and manage members** to add members to the group.

22. In the **Inside Sales** group window that appears, select **+ Add members**. This displays the list of active Microsoft 365 users.

23. In the list of users, select the check boxes for **Diego Siciliani** and **Lynne Robbins**, and then at the bottom of the window select **Save**.

24. Select **Close**. This displays the list of users for this group. Select **Close** again.

25. On the **Inside Sales** window, Diego and Lynne should now appear as members of the group. If they don't appear, select the **Refresh** icon in the upper right-hand corner of the window to refresh it (if they still don't appear, wait a minute or two and Refresh again). Once Diego and Lynne appear under the **Members** section, select the **X** in the upper right-hand corner to close the window.

26. Repeat steps 19-25 to add **Isaiah Langer**, **Megan Bowen**, and **Nestor Wilke** as members of the **IT admins** group.

27. You now want to test the effect of deleting a group. In the list of **Active groups,** select the vertical ellipsis icon (**More actions**) that appears to the right of the **Inside Sales** group. In the drop-down menu that appears, select **Delete group**.

28. In the **Delete Inside Sales?** pane that appears, select the **Delete group** button.

29. Once the group is deleted, select **Close**.

30. This will return you to the list of **Active groups** in the **Microsoft 365 admin center**. The **Inside Sales** group should no longer appear. If the Inside Sales group still displays, wait a couple of minutes and then select the **Refresh** option on the menu bar. The updated **Active groups** list should no longer include the Inside Sales group.

31. To verify whether deleting this group affected any of its owners or members, select **Users** and then **Active Users** in the left-hand navigation pane.

32. In the **Active users** list verify that the Inside Sales group's two owners (**Allan Deyoung** and **Patti Fernandez**) and the two members (**Diego Siciliani** and **Lynne Robbins**) still appear in the list of users. This verifies that deleting a group does not delete the user accounts that were owners or members of the group.

33. Remain logged into LON-DC1 with the **Microsoft 365 admin center** open in your browser for the next task.

6.0.3 Task 3 – Recover Groups using PowerShell

In this task, you will use Windows PowerShell to recover the Inside Sales group that you previously deleted. To use Windows PowerShell to perform this Azure AD-related task, the Windows Azure Active Directory PowerShell Module must be installed.

NOTE: You should have installed the Windows Azure Active Directory PowerShell Module in the prior lab exercise.

1. If you're not logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**, then please do so now.

2. If Windows PowerShell is still open from the previous exercise, select the **Windows PowerShell** icon on the taskbar; otherwise, you must open an elevated instance of Windows PowerShell just as you did before. Maximize your PowerShell window.

3. In **Windows PowerShell**, at the command prompt type the following command and then press Enter to connect with an authenticated account to use Active Directory cmdlet requests:

   ```
   Connect-AzureAD
   ```

4. A new window will appear requesting your credentials. Sign in using Holly's Microsoft 365 account of **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and **Pa55w.rd** as the Password.

5. At the command prompt, type the following command and then press Enter to display the repository of deleted groups (this should display the **Inside Sales** group that you earlier deleted):

```
Get-AzureADMSDeletedGroup
```

6. At the command prompt, either type or copy and paste in the following command; however, do not press Enter yet as you must first replace {objectId} with the actual Object ID of the deleted Inside Sales group.

```
Restore-AzureADMSDeletedDirectoryObject -Id {objectId}
```

After entering or copy and pasting in the command, you must replace {objectId} with the Object ID of the Inside Sales group that appears in the table of deleted groups that was displayed after you ran the command in the prior step. To do so, you must select the entire ID of the Inside Sales group and then copy it to the clipboard by pressing Ctrl-C. To paste in the object ID, place your cursor in the correct position in the command line where {objectId} should appear and then press Ctrl-V.

After pasting in the Object ID, press Enter to run the command. This will retrieve and restore the deleted group whose Object ID matches the value you entered.

NOTE: If nothing happens when you hit Enter, then extraneous hidden characters may have been pasted in following the object ID. If this occurs, retype the command and then after pasting in the object ID, hit the Delete key a couple of times to delete any extraneous characters that may have been pasted in following the object ID, and then press Enter again.

7. Leave your Windows PowerShell window open for the next exercise; simply minimize the PowerShell window for now.

8. You should now verify the **Inside Sales** group has been recovered. To do this, go to the **Microsoft 365 Admin Center** in your Edge browser, and then under **Groups** in the left-hand navigation pane, select **Active groups**.

9. Verify the **Inside Sales** group has been restored and is present in the list of active groups. If the Inside Sales group does not appear, wait a minute or two and then select **Refresh** on the menu bar above the list of groups.

10. You now want to verify that the recovery process correctly updated the group's membership. From the **Active groups** windows, select the **Inside Sales** group.

11. In the **Inside Sales** pane, select the **Members** tab. **Allan Deyoung** and **Patti Fernandez** should appear as owners of the group, and **Diego Siciliani** and **Lynne Robbins** should appear as members of the group.

12. Close the **Inside Sales** window.

13. Remain logged into LON-DC1 and leave your browser tabs open so that they're ready for the next task.

7 Proceed to Lab 1 - Exercise 3

8 Module 2 - Lab 1 - Exercise 3 - Add a Custom Domain

Not every company has just one domain; in fact, many companies have more than one domain. Adatum has just purchased a new domain (xxxUPNxxx.xxxCustomDomainxxx.xxx; the exact name of which is provided by your lab hosting provider) that resides in Microsoft Azure but not in Adatum's on-premises environment. To support Adatum's new custom domain, your lab hosting provider took on the role of Adatum's third-party domain registrar.

In this exercise, you will gain experience adding this domain to Adatum' Microsoft 365 deployment. When you add a domain to Microsoft 365, it's called an accepted, or custom domain. Custom domains allow companies to have their own branding on emails and accounts so that customers can verify who is emailing them (for example, @contoso.com). When a company adds a new domain to Microsoft 365, it must also maintain the DNS records that are necessary to support the services required by the company for the new domain.

Most companies do not personally manage their domains' 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.

That being said, for the purpose of this lab, you will be asked to manually create the necessary DNS records required by this new custom domain. In the other Microsoft 365 training courses that use a custom domain (such as MS-101T00 and MS-030T00), the custom domain and its DNS records will be added into Adatum's Microsoft 365 deployment by the lab hosting provider, who will take on the role of the third-party domain registrar for Adatum. However, this MS-100T00 training course will task you with adding the domain and creating its required DNS records so that you gain experience and understanding of what the DNS records are about and why they are required for a new domain.

8.0.1 Task 1 - Add a Custom Domain

In your hosted lab environment, Adatum already has an existing on-premises domain titled **adatum.com**, along with a Microsoft 365 domain titled **xxxxxZZZZZZ.onmicrosoft.com**. In this lab, you will create a second Microsoft 365 domain for Adatum that will be titled **xxxUPNxxx.xxxCustomDomainxxx.xxx**; you will replace **xxxUPNxxx** with the UPN name assigned to your tenant by your lab hosting provider, and you will replace **xxxCustomDomainxxx.xxx** with your lab hosting provider's custom domain name. Your instructor will provide you with your lab hosting's provider's custom domain name as well as show you how to locate the UPN name.

1. If you're not logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**, then please do so now.

2. If Windows PowerShell is still open from the previous exercise, select the **Windows PowerShell** icon on the taskbar; otherwise, you must open an elevated instance of Windows PowerShell just as you did before. Maximize your PowerShell window.

3. At the command prompt, you should run the following command to create a new zone in your on-premises DNS (remember to replace xxxUPNxxx with the unique UPN name assigned to your tenant by your lab hosting provider, and replace xxxCustomDomainxxx.xxx with your lab hosting provider's custom domain name):

   ```
   dnscmd /zoneadd xxxUPNxxx.xxxCustomDomainxxx.xxx /DsPrimary
   ```

4. Minimize your Windows PowerShell window (do NOT close it as you will use it later).

5. In your Microsoft Edge browser that was left open from the prior task, you should still be logged into Microsoft 365 as Holly Dickson. In the left-hand navigation pane in the **Microsoft 365 admin center**, select **...Show all**, select **Settings**, and then under the **Settings** group select **Domains**.

6. On the **Domains** page, note that in the list of domains, only the **xxxxxZZZZZZ.onmicrosoft.com** domain appears. The existing on-premises **adatum.com** domain does not appear in the list of Microsoft 365 domains. To add Adatum's new Microsoft 365 domain, select **+Add domain** in the menu bar that appears above the list of domains; this will start the **Add domain** setup wizard.

7. In the **Add a domain** page, in the **Domain name** field, enter your domain name in the form of **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx is the unique UPN name provided by your lab hosting provider, and xxxCustomDomainxxx.xxx is your lab hosting provider's domain name), and then select **Use this domain**.

8. In the **How do you want to verify your domain?** page, you must select a verification method to prove you own the domain. For this lab, select the **Add a TXT record to the domain's DNS records** option and then select **Continue**.

9. On the **Verify you own this domain** page, you must copy the **TXT value** (NOT the TXT name) so that you can configure the domain later on in DNS Manager. To do so, select the **Copy record** icon that appears to the left of the **TXT value** (to the left of **MS=msXXXXXXXX**). If a dialog box appears, select **Allow access** to copy this value from the webpage to your clipboard.

   Important: Do not select the **Verify** button at this point; instead, proceed to the next step. However, if you did select the **Verify** button, you will receive an error indicating the system could not find the record you added for this domain (you can do this if you want to see the error; there is no harm in it). Therefore, you must complete the next series of steps to add the TXT record to this domain in **DNS Manager**. Once you finish that process, you will be instructed to return back to this page and select the **Verify** button so that you can complete the process of adding this domain in the Microsoft 365 admin center.

10. Before you can verify you own this domain in the **Add domain** wizard, you must first add a DNS record for this domain in Server Manager. Select the **Server Manager** icon that appears in your taskbar at the bottom of the page. Maximize the Server Manager window if necessary.

11. In **Server Manager Dashboard,** select **Tools** in the top right corner of the window. In the drop-down menu that appears, select **DNS**, which will open **DNS Manager**. Maximize the DNS Manager window.

12. In the **DNS Manager** window, in the **File Explorer** section in the left-hand column, under **LON-DC1** expand the **Forward Lookup Zones** folder and then select the **xxxUPNxxx.xxxCustomDomainxxx.xxx** zone that you previously added in Windows PowerShell (where xxxUPNxxx is the unique UPN name provided by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's domain name).

13. Right-click on this **xxxUPNxxx.xxxCustomDomainxxx.xxx** zone, and in the menu that appears, select **Other New Records...**

14. In the **Resource Record Type** window that appears, in the **Select a resource record type** field, scroll down and select **Text (TXT),** and then select the **Create Record...** button at the bottom of the window.

15. In the **New Resource Record** box, in the **Text (TXT)** tab, leave the **Record name** field blank. However, right-click in the **Text** field and select **Paste** from the menu that appears. This will paste in the TXT valued of **MS=msXXXXXXXX** that you copied to the clipboard when you were in the Microsoft 365 admin center.

16. Select **OK** to create the record.

17. In the **Resource Record Type** window, select **Done**. Note how this Text (TXT) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created.

    Leave your **DNS Manager** window open but minimize it as you will return to it in a later step in this task. Minimize the **Server Manager** window as well.

18. You are now ready to return to the Microsoft 365 admin center and resume adding the domain record. If you'll recall, when you were earlier adding the domain in the Microsoft 365 admin center, you indicated that you wanted to verify the domain using a TXT record. At that point you had to switch to DNS Manger and add the TXT record. Now that you've added the TXT record, you can go back to the Microsoft 365 admin center and proceed with the domain verification process.

    In your Edge browser, you should be back in the **Microsoft 365 admin center** tab that displays the **Verify you own this domain** page. The **TXT name** should display your UPN name (xxxUPNxxx) and the **TXT value** should display your MS=msXXXXXXXX value.

19. Scroll to the bottom of the window and select **Verify.**

    Note: If you selected **Verify** in the prior step when you copied the TXT value just to see the error that you would receive, the **Verify** button changed to **Try again**. In you did this, then select **Try again** rather than **Verify**.

    Warning: It can sometimes take up 5 to 10 minutes for the change that you just made to propagate through the system, and sometimes it can take significantly longer depending on your registrar (in this case, your lab hosting provider). If you receive an error indicating the system could not detect the record that you added, wait 5 minutes and select the **Try again** button. Continue to do so every 5 minutes or so until the TXT record is successfully verified, at which point the **Activate records** window will appear.

    Important: If you had a typo or any other configuration mistakes, the domain will not be verified. If this occurs, the **How do you want to connect to your domain?** window in the next step will not appear. In this case, select the **Back** button to repeat this task. Take your time when configuring the domain to make sure you don't run into similar issues at this step in the process.

20. If your Text (TXT) record was successfully verified, the **How do you want to connect to your domain?** window will appear. Select **Continue**.

21. In the **Add DNS records** window, it enables you to add DNS records for three services that DNS supports - Exchange and Exchange Online Protection, Skype for Business, and Intune and Mobile Device Management for Microsoft 365.

Exchange and Exchange Online Protection is displayed by default and its check box is also selected by default. To see the other two services, select **Advanced Options**. Note that under **Advanced Options**, neither the **Skype for Business** nor the **Intune and Mobile Device Management for Microsoft 365** check boxes are selected. This is sufficient for Adatum; you should NOT select either of these two check boxes. Only the **Exchange and Exchange Online Protection** check box should be selected.

Under the **Exchange and Exchange Online Protection** service, the description indicates that 3 DNS records are needed for it to work properly: a Mail Exchanger (MX) record, an Alias (CNAME) record, and an additional Text (TXT) record. You must now switch back and forth between this **Add DNS records** page and **DNS Manager** to add these three additional DNS records for the new domain. For each DNS record that you add in DNS Manager, you will copy information from this **Add DNS records** page and then paste it into each corresponding record that you create in DNS Manager.

On the **Add DNS records** page, under the **Exchange and Exchange Online Protection** section, select the arrow ($>$) in the **MX Records** section to expand it. This displays the **Expected value** that the domain setup wizard expects to see in the MX record that you create for this domain in DNS Manager.

Then select the arrow ($>$) in the **CNAME Records** section and the **TXT Records** section. All three record types should now be expanded.

22. You will begin by adding the **MX record** required by the **Exchange and Exchange Online Protection** service.

    a. In the **MX Records** section, under the **Points to address or value** column, select the copy icon that appears to the left of the expected value (for example, xxxUPNxxx-xxxCustomDomainxxx-xxx.mail.protection.outlook.com) to copy this value to the clipboard. If a dialog box appears, select **Allow access** to allow the webpage to copy the value to the clipboard.

    b. You must now switch to DNS Manager. On the taskbar at the bottom of the page, select the **DNS Manager** icon.

    c. In **DNS Manager**, under **Forward Lookup Zones**, the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain should be selected from when you earlier left off. If not, select this zone now. You should see the **TXT** record that you created earlier. You must now create a **Mail Exchanger (MX)** record for this domain. Under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Mail Exchanger (MX)...**

    d. In the **New Resource Record** window, in the **Mail Exchanger (MX)** tab, leave the **Host or child domain** field blank, but right-click in the **Fully qualified domain name (FQDN) of mail server** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you copied to the clipboard in **step a** above.

    e. Select **OK**. Note how this Mail Exchanger (MX) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.

    f. Switch back to the **Add DNS records** page in the Microsoft 365 admin center by selecting the **Microsoft Edge** icon on the taskbar at the bottom of the page and selecting the **Microsoft 365 admin center** tab. At this point, you can either select **Continue** at the bottom of the **Add DNS records** page to verify the MX record that you just added, or you can wait until you have added all three records and then select **Continue** to verify all three records at once.

    For the purposes of this lab, you will verify each record as you create it. Therefore, select **Continue**. It will display either a checkmark or an exclamation point next to **MX Records**. The checkmark in a green circle indicates that it successfully validated the MX record for this domain in DNS Manager, and the exclamation point in a red circle indicates that there was a problem with the MX record and it did not validate successfully. If the MX record did not validate successfully, then review the record to ensure you entered the proper information, make any necessary corrections, and then select **Continue** again.

23. Once a checkmark appears next to **MX Records**, you must perform the following steps to add the **CNAME record** required by Exchange and Exchange Online Protection service.

    a. On the **Add DNS records** page, in the **CNAME Records** section, under the **Points to address or value** column, select the copy icon that appears to the left of the expected value (for example, autodiscover.outlook.com).

Important: You will NOT copy the expected **Host Name** value. The value listed here as the expected host name is **autodiscover.xxxUPNxxx** (where xxxUPNxxx is your UPN name). However, if you paste this value in the **Alias name** field in the CNAME record in DNS Manager, the CNAME record validation on this page will fail. When you create the CNAME record in DNS Manager in the following steps, you will simply enter **autodiscover** as the **Alias name** and NOT **autodiscover.xxxUPNxxx**.

The reason for using only **autodiscover** as the **Alias name** is that Autodiscover is an Exchange service that minimizes configuration and deployment. For small, single SMTP namespace organizations such as Adatum, only autodiscover is needed as the Alias, as opposed to autodiscover.xxxUPNxxx for larger organizations with multiple SMTP namespaces. By adding the CNAME record to your on-premises DNS server, you're creating a redirect record that allows users to configure Outlook and access OWA by using either Basic Authentication or Modern Authentication(OAUTH).

Therefore, the only value you need to copy for the CNAME record is the expected value for the **Points to address or value** column (for example, autodiscover.outlook.com).

b. On the taskbar at the bottom of the page, select the **DNS Manager** icon.

c. In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Alias (CNAME)...**

d. In the **New Resource Record** window, enter **autodiscover** in the **Alias name (uses parent domain if left blank)** field.

e. Right-click in the **Fully qualified domain name (FQDN) for target host** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you earlier copied to the clipboard.

f. Select **OK**. Note how this Alias (CNAME) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.

g. Switch back to the **Add DNS records** page in the Microsoft 365 admin center. On the taskbar at the bottom of the page, select the **Microsoft Edge** icon and select the **Microsoft 365 admin center** tab. At this point, you can either select **Continue** at the bottom of the **Add DNS records** page to verify the CNAME record, or you can wait until you have added all three records and then select **Continue** to verify all three records at once.

For the purpose of this lab, select **Continue**. It will display either a checkmark or an exclamation point next to **CNAME Record**. The checkmark in a green circle indicates that it successfully validated the CNAME record for this domain in DNS Manager, and the exclamation point in a red circle indicates that there was a problem with the CNAME record and it did not validate successfully. If the CNAME record did not validate successfully, then review the record to ensure you entered the proper information, make any necessary corrections, and then select **Continue** again.

24. Once a checkmark appears next to **CNAME Records**, you will finish by adding the **TXT record** required by Exchange and Exchange Online Protection service.

a. On the **Add DNS records** page, in the **TXT Records** section, under the **TXT value** column, select the copy icon that appears to the left of the expected value (for example, v=spf1 include:spf.protection.outlook.com -all) to copy this value to the clipboard.

b. On the taskbar at the bottom of the page, select the **DNS Manager** icon.

c. In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **Other New Records...**

d. In the **Resource Record Type** window that appears, in the **Select a resource record type** field, scroll down and select **Text (TXT),** and then select the **Create Record...** button at the bottom of the window.

e. In the **New Resource Record** window, in the **Text (TXT)** tab, leave the **Record name** field blank. However, right-click in the **Text** field and select **Paste** from the menu that appears. This will paste in the expected **TXT value** that you earlier copied to the clipboard.

f. Select **OK**.

g. On the **Resource Record Type** window, select **Done**.

25. In **DNS Manager**, you should now see the TXT record that you originally created to verify the domain, along with the MX, CNAME, and TXT records that you created for the Exchange service to work within this domain.

   Minimize the DNS Manager window.

26. This should return you to the **Add DNS records** window in your Edge browser. Select **Continue** to complete the new domain setup. If you selected **Continue** after adding the MX and CNAME records, and if each validated successfully, then only the TXT record will be validated at this point. However, if you did not select **Continue** after adding the MX and CNAME records, then all three records will be validated at this point.

   If all three records have been successfully validated, then the **Domain setup is complete** page will appear. If this occurs, then select the **Done** button to complete the domain setup process.

   However, if any of the three records did not validate successfully, then the **Add DNS records** window will return, and it will display either a checkmark or an exclamation point next to each record type to indicate which ones validated successfully and which ones did not. An exclamation point in a red circle indicates that there was a problem with the record and it did not validate successfully (note that the Actual value for the record is left blank). If this occurs, you must correct the data on the corresponding record in DNS Manager and then select **Continue** again. You must repeat this process until all three records have successfully validated and the **Domain setup is complete** page appears.

27. Once the domain setup process is complete and the three DNS records validated successfully for the **Exchange and Exchange Online Protection** service, the **Domains > xxxUP-Nxxx.xxxCustomDomainxxx.xxx** page will be displayed. Verify the **Domain status** is **Healthy**.

28. On the **Domains > xxxUPNxxx.xxxCustomDomainxxx.xxx** page, select the **Domains** portion of this thread. The **xxxUPNxxx.xxxCustomDomainxxx.xxx** custom domain that you just added should now appear in the list of domains, along with your **xxxxxZZZZZZ.onmicrosoft.com** domain.

29. Remain logged into the LON-DC1 VM with both **Microsoft Edge** and **Windows PowerShell** left open for the next task.

9   End of Lab 1

10   Module 3 - Lab 2 - Exercise 1 - Manage Administration Delegation

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 the Microsoft 365 user accounts that were created by your lab hosting provider. You will assign these roles using both the Microsoft 365 admin center and Windows PowerShell; this will give you the added experience of 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.

10.0.1   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 LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**, then please do so now.

2. In the **Microsoft 365 admin center** in your Edge browser, you should still be logged in as Holly Dickson. In the left-hand navigation pane, select **Users** and then select **Active Users**.

3. In the **Active users** list, select **Diego Siciliani**.

   Note: Select Diego's name; do not select the circle to the left of his name. The circle with the check mark is typically used for selecting multiple users when you want to perform one of the user-related actions on the menu bar that appears above the list of users, such as **Manage product licenses** and **Manage roles**. Selecting a user's name opens a detail pane specifically for that user.

4. In the **Diego Siciliani** pane that appears, the **Account** tab is displayed by default. In this tab, 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 by 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 are sorted 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 Administrator** role under the **Identity** category.

   Note: Both roles are in the list of commonly used admin roles that appear under the **Admin center access** option; therefore, you do not have to select **Show all by category**.

10. Remain logged into LON-DC1 and the Microsoft 365 admin center as Holly Dickson.

10.0.2 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 Microsoft 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 Microsoft 365 deployment. In this task, you will learn how to use PowerShell to display all the users assigned to a specific role.

1. On LON-DC1, select the Windows PowerShell icon on the taskbar 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 connecting your PowerShell session to the Microsoft Online Service. At the command prompt, type the following command, and then press Enter:

   ```
   Connect-MsolService
   ```

3. In the **Sign in** dialog box that appears, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix 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. 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. This displays a window that shows all the Microsoft 365 roles. Notice how the "official" name of all roles within Microsoft 365 includes the complete spelling of the word "administrator"; whereas, in the Microsoft 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.

   Close the window displaying the Microsoft 365 roles.

7. Holly now wants to assign **Patti Fernandez** to the **Service support administrator** role. In the Windows PowerShell window, at the command prompt, type the following command (don't forget to

replace xxxxxZZZZZZ with the tenant prefix provided by your lab hosting provider), and then press Enter:

Add-MsolRoleMember -RoleName "Service support administrator" –RoleMemberEmailAddress PattiF@ xxxxxZZZZZZ.onmicrosoft.com

8. 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

9. 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
   ```

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

11. 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
    ```

12. 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).

13. Leave your Windows PowerShell session open for future lab exercises; simply minimize it before going on to the next task.

10.0.3   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, 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@xxxxxZZZZZZ.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. In your VM lab environment, switch to the Client 1 VM (**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. Maximize your Edge browser window if necessary.

11. In your **Edge** browser navigate to **https://portal.office.com**.

12. You will begin by signing into Microsoft 365 as **Allan Deyoung**. In the **Sign-in** window, enter **AllanD@ xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). In the **Enter password** window, enter the Tenant Password provided by your instructor. If you are signed in to another account, sign out and sign back in using **Allan Deyoung** credentials .

13. On the **Stay signed in?** window, select the **Don't show this again** check box and then select **Yes**.

14. If a **Get your work done with Office 365** window appears, select the **X** to close it.

15. In the **Office 365 Home** page, note how the **Admin** option is not available in the column of app icons on the left side of the screen since Allan was never assigned an administrator role.

16. You will now sign out of Microsoft 365 as Allan. In **Microsoft Edge**, at the top right of the **Office 365 home** page, select the user icon for **Allan Deyoung** (the circle in the upper right-hand corner with Allan's picture in it), and in the **Allan Deyoung** window that appears, select **Sign out.**

17. You will now sign into Microsoft 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@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Sign in**. In the **Enter password** window, enter the Tenant Password provided by your instructor.

18. If a **Get your work done with Office 365** window appears, select the **X** to close it.

19. In the **Office 365 home** page, note how the **Admin** icon appears in the column of app icons on the left side of the screen; this is because Lynne was assigned to a Microsoft 365 administrator role. Select the **Admin** icon to open the Microsoft 365 admin center.

20. In 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**, who each 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, if the **Automatically create a password** check box displays a check mark, then select this box to clear it. This will enable Lynne to manually assign Diego a password. Enter **diego** in the **Password** field. Note to the right of the password, the system displays a message indicating this is a **Weak** password. Also note the message that appears below the field indicating the requirements for a strong password. Finally, note how the **Reset password** button at the bottom of the pane is not enabled; this button will only be enabled once you enter a strong password.

    To correct this situation, enter **P@$$w0rd** in the **Password** field. Note how **Strong** now appears next to this password, and the **Reset password** button at the bottom of the pane is now enabled.

Note: This is just a temporary password because Lynne wants to force Diego to change it the next time he logs in. Therefore, verify the **Require this user to change their password when they first sign in** check box displays a check mark; if the box is clear, then select it so that it displays a check mark.

23. Select **Reset password**.

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, and because Lynne is not a Global admin, she will have 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, if the **Automatically create a password** check box displays a check mark, then select this box to clear it. Lynne wants to manually assign Allan a password, so enter **P@$$w0rd** in the **Password** field.

    This is just a temporary password because Lynne wants to force Allan to change it the next time he logs in. Therefore, verify the **Require this user to change their password when they first sign in** check box displays a check mark; if the box is clear, then select it so that it displays a check mark.

28. Select **Reset password**.

29. On the **Reset password** window, you should receive a message indicating the password was successfully reset. Select the **Email the sign-in info to me** check box. This displays a **Your email** 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 in this field, they must be separated by a semicolon and a space. Therefore, enter a semicolon and a space following Lynne's email address, enter Allan's email address of **AllanD@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the prefix 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: Since you are going to run a global command on Alex's account rather than a command associated with his account, you only want Alex's account selected in the list of active users. If any other user account is selected, you must unselect that user account before proceeding. Examine Allan Deyoung's account, since you just reset his password; uncheck his account if necessary (select the check mark to unselect it). 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, verify Alex's email address appears below the window heading. Select the **Block this user from signing in** check box, and then select **Save changes.**

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.

    Close the **Block sign-in** window.

36. You previously blocked Alex Wilber from being able to sign in. To verify whether he is blocked, 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 the **Lynne Robbins** window that appears, 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@ xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). In the **Enter password** window, enter the Tenant Password provided by your instructor.

    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**.

    Note the warning message that's displayed indicating it can take up to 15 minutes before Alex can sign in again. As such, you will **NOT** try to log back in as Alex on LON-CL1. Instead, remain on LON-DC1 and simply close the **Unblock sign-in** window.

41. On LON-DC1, leave your browser and all tabs open and proceed to the next exercise.

11 Proceed to Lab 2 - Exercise 2

12 Module 3 - Lab 2 - Exercise 2 - Monitor and Troubleshoot Microsoft 365

In this exercise you will be introduced to some troubleshooting tools in Microsoft 365 that enable you to troubleshoot mail flow issues. You will then analyze Adatum's Microsoft 365 service health by reviewing several of the key service health queries and reports that are available in Microsoft 365. You will conclude this exercise by reviewing how to submit a service request with the Microsoft Support team should you ever need assistance with a problem.

12.0.1 Task 1 - Troubleshoot Mail Flow in Microsoft 365

Holly Dickson, Adatum's new Enterprise Administrator, wants to prepare herself for any potential mail flow problems that may occur within Adatum's Exchange environment. As part of her pilot project, she has decided to create two test scenarios to analyze some of the troubleshooting options available to her. One email will be sent to an email address with an invalid domain (@alt.none), and another will be sent to an address with an invalid mailbox in a valid domain (@outlook.com). This task guides Holly though a variety of tools that she can use to troubleshoot different mail conflict scenarios.

1. You should still be logged into LON-DC1 after having completed the prior exercise, and you should still be logged into Microsoft 365 as Holly Dickson.

2. In your **Microsoft Edge** browser, select the **Microsoft Office Home** tab to display the Office 365 Home page, which should still be open (if not, navigate to **https://portal.office.com** and log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and **Pa55w.rd**).

3. In the **Office 365 Home** page, select the **Outlook** icon in the column of app icons on the left.

    Note: If an **Outlook settings** window appears, accept **English** as the language, select your corresponding **Time zone**, and then select **Save**.

4. If a **Pick an account** window appears, select Holly's account of **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZis the tenant prefix provided by your lab hosting provider), and then enter **Pa55w.rd** in the **Enter password** window and select **Sign in**.

5. Holly's **Inbox** will be displayed in Outlook. If a **Welcome** window appears, select the **X** in the upper-right corner of the window to close it.

   In Holly's mailbox, at the top of the left-hand navigation pane, select the **New message** button to create a new email.

6. In this email, you will send the mail to an email address in which the domain (alt.none) is an invalid domain. In the email pane that appears, enter **user@alt.none** in the **To** field . After entering the email address, tab off the **To** field to commit the entered value.

7. Enter a subject and some body text and then send the email.

8. Wait for the delivery failure message to appear in Holly's Inbox, then double-click the message to open it in a new window. This will make it easier to copy the text of the message in the next step.

9. In the message window, scroll down through the message until you reach the body of text that says **Diagnostic information for administrators**. Select the text in the body of the message starting after **Diagnostic information for administrators** through the end of the message. With this text selected, press **Ctrl+C** to copy it to the clipboard, and then close message window.

10. Open a new tab in your web browser and enter the following URL in the address bar: **https://testconnectivity.micros**

11. This opens the **Microsoft Remote Connectivity Analyzer** portal. In the navigation bar on the left, select the **Message Analyzer** tab. This opens the **Message Header Analyzer** tool.

12. Take a moment to review the **Message Header Analyzer** tool. It consists of two sections - In the top section, you will paste in the diagnostic data that you copied from the failure to deliver email message; in the bottom section, the tool will display its analysis of this data.

13. In the **Message Analyzer Header** window, paste the message (right-click and select **Paste**, or press **Ctrl+V**) in the field that appears below the **-Insert the message header you would like to analyze** row, and then select the **Analyze headers** button.

14. SMTP message headers contain a wealth of information that allow you to determine the origins of a message and how it made its way through one or more SMTP servers to its destination. Here's a quick summary of the information found in this header analysis:

   - **Summary section**: Displays the most important properties and total delivery time at a quick glance. Depending on the diagnostic data (for example, if a message was even sent), this section may or may not appear.

   - **Received headers section**: Displays the more important header properties and delivery time. Enables you to analyze the received headers and displays the longest delays quickly for each discovery of sources of message transfer delays.

   - **Other headers section**: Enables you to quickly detect where the longest message transfer delays occurred. You can sort all headers by occurrence number, name or value.

   The primary problem in this example (see the **Other headers** section, Hop 1) is that the DNS domain of the email address (**@alt.none**) does not exist. Normally this is caused by a typo in the recipient's domain name that needs to be corrected to resolve the issue.

15. Select the **Clear** option that appears to the right of the **Analyze headers** button; this will reset the Message Header Analyzer window.

16. Return to the **Mail - Holly Dickson - Outlook** tab in your browser. In Holly's mailbox, select **New message** to create a new email.

17. In this email, you will send the mail to a non-existent mailbox in a valid domain (outlook.com). In the **To** field, enter an email address of **{a random series of numbers followed by your name}@outlook.com** (for example, 123456LynneRobbins@outlook.com). After entering the email address, tab off the **To** field to commit the entered value.

18. Enter a subject and some body text and then send the email.

19. Wait for the delivery failure (NDR) message to appear in Holly's Inbox, then double-click the message to open it in a new window.

Note: When this lab was originally written, it asked the student to enter difflop8675399@outlook.com in the **To** field. The lab author never assumed anyone would ever create a mailbox called **difflop8675399** in the outlook.com domain. This worked fine for several months, until someone actually created this mailbox in outlook.com. This broke the lab, since it stopped returning an NDR reply. So the previous instruction was changed to ask you to send this email to an email address consisting of a random series of numbers followed by your name. Hopefully, the combination you choose is not a valid mailbox. **If you do not receive an NDR reply within a minute (or less) after sending the email, then you can assume someone has created that mailbox in the outlook.com domain.** If this occurs, then send another email to a different mailbox address that you feel is completely bogus.

20. In the window for the NDR reply, scroll down through the message until you reach the body of text that says **Diagnostic information for administrators**. Select the text in the body of the message starting after **Diagnostic information for administrators** through the end of the message. With this text selected, press **Ctrl+C** to copy it to the clipboard, and then close the message window.

21. Switch to the **Message Header Analyzer** tab in your browser.

22. In the **Message Analyzer Header** window, paste the message in the field that appears below the **-Insert the message header you would like to analyze** row, and then select **Analyze headers**.

    Note: Review the diagnostic information and the time taken for the message to be rejected. In the prior email, the domain of the email address did not exist. In this email, the user's domain (outlook.com) was valid, but the user mailbox was unavailable.

23. Close both the **Message Header Analyzer** tab and the **Microsoft Remote Connectivity Analyzer** tab in your Edge browser.

24. If the **Microsoft 365 admin center** tab is still open in your browser, then select that now; otherwise, select the **Microsoft Office Home** tab in your Edge browser and then select the **Admin** icon.

25. On the **Microsoft 365 admin center** page, in the left-hand navigation pane, select **Show all** (if necessary).

26. Scroll down through the left-hand navigation pane, and under **Admin centers,** select **Security**. This will open the Office 365 Security & Compliance center in a new tab.

27. In the **Office 365 Security & Compliance center**, in the left-hand navigation pane, select **Mail flow**, and then in the Mail Flow group, select **Message trace**.

28. In the **Home > Message trace** window, select the **+Start a trace** button.

29. In the **New message trace** pane that appears, select the **By these people** field. This displays the list of active users. Scroll down and select **Holly Dickson**.

30. Under the **Within this time range** section, select **1 day** that appears above the slider. Note how the slider circle moved under **1 day**.

31. Scroll down and select **More search options**. In the **Delivery status** field, select the drop-down arrow and select **Failed**.

32. At the bottom of the page, select the **Search** button.

33. In the **Message trace search results** window that appears, if no failed message deliveries appear in the list, you may need to wait several minutes before selecting the **Refresh** button that appears above the item list.

34. Double-click on the first failed message to view the **Message trace details** pane for that message. This displays the sender, recipient, status, and error information, as well as the **How to fix it** instructions. Select the **Close** button at the bottom of the pane to close it.

    Repeat this step for the other failed message.

35. Close the **Message trace search results** window, and then close the **New message trace** window. This will return you to the **Home > Message trace** window in the **Office 365 Security and Compliance center**. Leave this tab open for the next task.

36. In your Edge browser, close the **Mail - Holly Dickson - Outlook** tab, but leave the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab open for the next task.

12.0.2 Task 2 - Monitor Service Health and Analyze Reports

Adatum's CTO is concerned with the service health issues that have recently come to light throughout the organization. He has asked Holly to review several of the key service health queries and reports so that she becomes aware of the information that's available to help Adatum monitor its service health.

1. On the LON-DC1 VM, select the **Microsoft 365 admin center** tab within your Edge browser.

2. In the left-hand navigation pane, you previously selected the **Show all** option in the prior task. Select the **Health** group that displayed when you selected **Show all**, and then select **Service health**.

3. On the **Service health** page, the **All services** tab is displayed by default across the top of the page. Select the **History** tab.

4. The default option is to display a list of items from the past 7 days (see the right side of the menu bar above the list of items; **Past 7 days** displays as the default option). Select any entry in the list to see further details about the incident. Close the incident window when you're done reviewing it.

5. In the **Microsoft 365 admin center**, on the left-hand navigation pane, select **Reports**, and then select **Usage.**

6. On the **Usage** page, scroll down and view the **Active users - Microsoft 365 Services** chart.

7. To the right of this chart, view the **Email activity** chart.

   Note: There may be little or no data shown due to the limited mailbox usage in the lab environment.

8. Under the **Email activity** chart select the **View more** button. This displays the **Email activity** report. In the report header at the top of the page, select the **Exchange activity** drop-down arrow. In the menu that appears, select the **Exchange** drop-down arrow and then select **Mailbox usage**.

9. The default mailbox usage that is initially displayed is **30 days**. Select the other date views at the top of the report (**7 days**, **90 days**, and **180 days**) to see how the display changes.

10. Scroll down to the bottom of the page to see mailbox details for each of the active users.

11. Scroll back to the top of the page. On the menu bar above the chart, it currently displays **Mailbox usage** followed by a drop-down arrow. Select the drop-down arrow, and in the menu that appears, select **SharePoint**. In the SharePoint group, select **Site usage**.

12. The default site usage that is initially displayed at the top-right of the screen is **Past 30 days**. Select the drop-down arrow next to this and in the menu that appears, select the other date views to see how the display changes: **7 days**, **90 days**, and **180 days**.

13. Scroll down to the bottom of the page to see details for each of the site collections for your tenant.

14. You now want to review the reports that are available in the **Office 365 Security & Compliance** center. In your browser, you should have the **Message trace - Security & Compliance** tab open from the prior task; if so, select it now. However, if you previously closed this tab, then in the **Microsoft 365 admin center**, under the **Admin centers** group, select **Security**.

15. In the **Office 365 Security & Compliance** center, scroll down in the left-hand navigation pane and select **Reports,** and then under the **Reports** section, select **Dashboard.**

16. In the **Home > Dashboard** window, scroll down to any report that has data displayed (for example, **Top senders and recipients**) and click in the chart area to open the **Report Viewer** for that report.

17. After reviewing the report, select **Dashboard** in navigation thread at the top of the page (Home > **Dashboard** > Report Viewer - Security & Compliance) to return to the report dashboard.

18. Repeat the prior two steps for any other report that has data displayed.

19. Close the **Security & Compliance center** tab in your Edge browser but leave the other Microsoft 365 admin center tabs open for the next task.

12.0.3 Task 3 – Submit a Help Request to Microsoft Support

If an organization runs into a situation in Microsoft 365 where it needs assistance with a problem, it must submit a service request with the Microsoft Support team. As part of Adatum's pilot project, Holly Dickson and Patti Fernandez (Adatum's Service Support Administrator) have decided to submit a test request that does not require a call back. They are performing this task to become familiar with the service request process.

1. On LON-DC1, in the **Microsoft 365 admin center** tab of your Edge browser, select **Support** in the left-hand navigation pane, and then select **View service requests** to see if there are any outstanding service request tickets. You should verify that no service request tickets appear on the **Service request history** page.

2. In the left-hand navigation bar, under the **Support** group, select **New service request**.

3. In the **Support Assistant** pane that appears, select the **Message** line at the bottom of the window (which currently displays **Message e.g. How do I install Office?**) and type the following message: **This is a test of the service request system; a call back is not needed.** When you are done, select the **Send message** arrow icon that appears below the message line.

4. This initiates an automated bot that asks a clarifying question and provides some optional answers that you can choose from. Select one of the answers to see how the automated bot responds.

5. If you need further assistance and would like to speak to a Microsoft support agent, at the top of the window select the **headset** icon (the middle icon) to get help from one of the support agents. Select the **headset** icon now.

6. In the **Contact support** window that appears, do NOT enter any information; instead, just review the information that you would enter to complete this request in a real-world situation. You could also attach any necessary documents before selecting **Contact me** at the bottom of the page.

   IMPORTANT: Do NOT complete this form in your lab environment. If you enter this request with the **Phone** option selected, you will receive a call from a Microsoft 365 support representative.

7. Select the **X** in the upper right-hand corner of the page to close the **Contact support** window.

8. Leave LON-DC1 and your Edge browser open for the next lab exercise.

13 Proceed to Lab 2 - Exercise 3

14 Module 3 - Lab 2 - Exercise 3 - Manage a Microsoft 365 Apps for enterprise installation

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 Office 365 deployment tool, 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.

14.0.1 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 (xxxxxZZZZZZ.onmicrosoft.com accounts); they do not have corresponding on-premises accounts in the adatum domain. Without an on-premises account, you cannot log into the Client 1 (LON-CL1) 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 on-premises domain (adatum.com) by your lab hosting provider. For this test, you will use **Laura Atkins**. You will create a Microsoft 365 account for Laura, but you will not assign her an Office 365 license.

1. You should still be logged into LON-DC1 as **Administrator** and password **Pa55w.rd**.

2. The **Microsoft 365 admin center** should still be open in your Edge browser from the prior lab, where you should be logged into Microsoft 365 as Holly Dickson. In the left-hand navigation pane, select **Users** and then select **Active users**.

3. 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**. Your lab hosting provider has already created an on-premises user account for Laura, but she does not have a Microsoft 365 user account. You will create a Microsoft 365 account for Laura, but you will not assign her an Office 365 license.

   At the top of the **Active users** window, select **Add a user** on the menu bar and select **Single user**.

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

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

   IMPORTANT: To the right of the Username field is the domain field. You want this value to be Adatum's **xxxxxZZZZZZ.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). However, if the custom domain that you added in a prior lab is set as the default domain, then this field will be prefilled with the custom **xxxUPNxxx.xxxCustomDomainxxx.xxx** on-premises domain (where xxxUPNxxx is your UPN number and xxxCustomDomainxxx.xxx is the custom domain). If the custom domain is displayed in this field, you must select the drop-down arrow and select the **xxxxxZZZZZZ.onmicrosoft.com** cloud domain instead.

   After configuring this field, Laura's **Username** should appear as: **Laura@xxxxxZZZZZZ.onmicrosoft.com**

   - Password settings: deselect the **Automatic create a password** option
   - Password: **Pa55w.rd**
   - Clear (uncheck) the **Require this user to change their password when they first sign in** check box

5. Select **Next**.

6. In the **Assign product licenses** window, select the **Create user without product license (not recommended)** option, and then select **Next**.

7. In the **Optional settings** window, select **Next**.

8. 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 looks good, select **Finish adding**.

9. On the **Laura Atkins added to active users** page, select **Close**. If a survey form appears, select **Cancel**.

10. Switch to the Client 1 VM (**LON-CL1**).

11. You want to log in as **Laura Atkins**. If the Edge browser is still open from the previous lab exercise, then close it now. You should be on the LON-CL1's desktop, where it should indicate that you are logged on as **adatum\administrator**. Since you want to log on as Laura Atkins, select the **Ctrl+Alt+Delete** function for your VM environment. On the menu screen that appears, select **Switch user**.

    The lower-left portion of the desktop displays the **Administrator** and **Other user** options. Select **Other user**.

12. In the **Other user** log in, enter **adatum\laura** in the **Username** field, enter **Pa55w.rd** as the **Password**, and then select the forward arrow to log in. After logging in, the desktop should indicate the logged on user is **adatum\laura**.

13. Select the **Microsoft Edge** icon on the taskbar.

14. 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/**

15. In the **Sign in** window, enter **Laura@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**.

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

17. In the **Stay signed in?** window, select the **Don't show this again** check box and then select **Yes.**

18. In the **Microsoft Office Home** page for Laura, notice that no column of Microsoft 365 app icons appears on the left-side of the screen; this is because Laura does not have an Office 365 license assigned.

    Select the **Install Office** button, and then in the drop-down menu that appears, select **Install software**. This opens the **My account** window for Laura.

19. In Laura's **My account** window, under the **Office apps & devices** section, select **View apps & devices**. 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.

20. Leave LON-CL1 open and remain signed into Microsoft 365 as Laura Atkins for the next task.

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

Holly is now going to test whether 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 back to **LON-DC1**. You should still be logged into Microsoft 365 as Holly Dickson, Adatum's Enterprise Administrator.

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 installation options**.

4. In the **Office installation options** pane that appears, under the **Apps for Windows and mobile devices** section, 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**.

6. Scroll to the top of the **Office installation options** pane. 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're once again going to use **Laura Atkins**, so you must first assign Laura an Office 365 license.

    In the **Microsoft 365 admin center**, under **Users** in the left-hand navigation pane select **Active users**, and then in the in the **Active users** list, scroll down to **Laura Atkins**. The value in the **Licenses** column for Laura currently indicates that she is **Unlicensed**. Select **Laura Atkins**.

8. In Laura Atkins' account window, the **Account** tab is displayed by default. Select the **Licenses and Apps** tab. In the **Licenses** section, select the **Office 365 E5** check box and then select **Save changes**. You can then close Laura's account window. In the **Active users** list, note how the value in the **Licenses** column for Laura now displays **Office 365 E5**.

9. You should now check whether Laura can download Microsoft 365 Apps for enterprise on to her client PC when the global Office download setting has been turned Off.

    To do this, you must first switch back to **LON-CL1**.

10. In **LON-CL1**, your Edge browser should still be open, and you should still be logged into Microsoft 365 as Laura Atkins. The **My account** window should be displayed, and the **Apps and devices** section should still be displayed along with the error message that you received in the prior task that indicated Laura was not assigned an Office license.

    Select the **Refresh icon** that appears to the left of the address bar at the top of your browser. This will refresh the **Office apps & devices** page.

Note: Refreshing the **Office apps & devices** page does not re-verify Laura's licensing status as it still returns the same error message as before when Laura was unlicensed. You were asked to refresh this page to show you this condition. Therefore, proceed to the next step to log out of Microsoft 365 and log back in as Laura.

11. Select the Laura Atkins icon (the circle with **LA** in it) in the upper-right corner of the screen, and in the **Laura Atkins** window that appears, 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.

12. In **Microsoft Edge**, 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/**

13. In the **Pick an account** window, select **Laura@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

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

15. In the **Stay signed in?** window, select the **Don't show this again** check box and then select **Yes.**

16. In the **Microsoft Office Home** page for Laura, notice that the column of Microsoft 365 app icons now appears on the left-side of the screen because Laura has been assigned an Office 365 license.

    Select the **Install Office** button, and then in the drop-down menu, select **Install software**.

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

18. In the **Apps & devices** window, a message is displayed under the **Office** section that indicates 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.

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

    To do this, switch back to **LON-DC1**.

20. On **LON-DC1**, you should still be logged into Microsoft 365 as Holly Dickson. In the **Microsoft 365 admin center**, under the **Settings** section in the left-hand navigation pane, select **Org Settings**.

21. In the **Settings** window, the **Services** tab is displayed by default. Scroll down through the list of services and select **Office installation options**.

22. In the **Office installation options** pane, 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.

23. Select **Save**.

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

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

    To do this, switch back to **LON-CL1**.

26. On **LON-CL1**, Laura's Edge browser should still be open, and the **Office 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 global option back On, you need to refresh this page to see how it affects Laura's ability to download Microsoft 365 Apps for enterprise.

    Note: Unlike the previous time when you refreshed this page and it did not reflect Laura's updated Office 365 license status, refreshing this page after updating the global download setting works.

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

27. In the **My account** window that appears, under the **Office apps & devices** section, an **Install Office** button 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.

28. Remain on LON-CL1 and continue to the next task to perform the user-driven installation for Laura Atkins.

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

In the prior task, you logged into Laura Atkins' client PC, and you verified that she could download Microsoft 365 Apps for enterprise once 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 Laura perform a user-driven installation of the Microsoft 365 Apps for enterprise suite from the Microsoft 365 portal.

1. On **LON-CL1**, you should still be logged in as Laura Atkins.

2. You should still be in Laura'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 Laura 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 Laura 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**.

4. In the notification bar that appears at the bottom of the page, select **Save** to download the 64-bit Microsoft 365 Apps for enterprise installation wizard to the client PC.

5. Once the Microsoft 365 Apps for enterprise installation file has finished downloading, select **Run** in the notification bar that appears at the bottom of the page.

6. If a **Do you want to allow this app to make changes to your device?** dialog box appears, enter **adatum\administrator** in the **username** box, type **Pa55w.rd** in the **Password** box, and then select **Yes**.

7. You may receive a **Continuing could be expensive** dialog box that displays a warning message indicating that it may be expensive to continue downloading because you're connected to a network that limits downloads every month.

   Important: If you receive this dialog box, it may appear in the taskbar but not on the desktop. If this occurs, hover your mouse over the **Office** icon on the taskbar, and then select the **Continuing could be expensive** dialog box if it appears. If you do receive this dialog box, the Office install will NOT proceed until you select **Continue** (the Office window will just keep displaying the **We're getting things ready** message, but it won't actually do anything).

   In the **Continuing could be expensive** dialog box, select **Continue**.

8. The installation may take several minutes to complete. Once the installation finishes, select **Close** in the **You're all set! Office is installed now** window.

9. To validate Laura'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 enterprise apps that were just installed. This should include Word, PowerPoint, OneNote 2016, Outlook, Publisher, Access, Skype for Business, and Excel.

10. In the **Start** menu, select **Word**.

11. On the **Sign in to set up Office** page, sign in as **Laura@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**.

12. On the **Accept the license agreement** window, select **Accept**.

13. On the **Your privacy option** window, select **Close**.

14. Verify that Word is functioning properly by opening a blank Word document, entering some text, and saving the document to the **Documents** folder.

15. Close Word.

16. Now that you have completed this lab exercise by installing Microsoft 365 Apps for enterprise, you should log out of LON-CL1 as Laura Atkins and log back in as the Adatum administrator. This will prepare LON-CL1 for the next lab.

    On LON-CL1, select the **Ctrl+Alt+Delete** function in your VM lab environment.

17. On the desktop menu, select **Switch user**.

18. On the desktop, the **Administrator** is selected by default. Enter **Pa55w.rd** in the **Password** field and then select the forward arrow.

    The desktop should now display the logged on user as **adatum\administrator**. LON-CL1 is now ready for the next lab.

15   End of Lab 2

16   Module 4 - Lab 3 - Exercise 10 - Build a Power BI report and dashboard

Holly Dickson is nearing the end of her excursion into the Microsoft Power Platform environment. She has built two Power Apps and a Power Automate Flow, all based on the Service Desk Ticketing system she created earlier in SharePoint.

She is now interested in building and sharing a Power BI report and dashboard based on the SharePoint ticketing system as well. Adatum's IT Consultant has suggested that she use Power BI Desktop, which is a free application that she can install locally that will let her connect to, transform, and visualize the ticketing system data. She can then use Power BI Desktop to create reports, and then use the Power BI service to share her reports with others.

In your role as Holly Dickson, you will use this exercise to create some basic visualizations for a Power BI report; the visualizations will be based on the **Service Desk Requests** list in the SharePoint team site titled **IT Services**.

16.0.1   Task 1: Create a Power BI report

In this task, you will download and install the Microsoft Power BI Desktop. Once installed, you will create a Power BI report based on the new Service Desk Ticketing system that you created earlier in SharePoint.

1. After having completed the prior lab exercise in which you created a Power Automate flow, you should still be logged into LON-CL1 as the **Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. In your Edge browser, make sure that your new Service Desk Ticketing system is open in a tab. The tab should be titled **IT Services − Service Desk Requests − All Items**. If you do not have this tab open, then go to the **SharePoint admin center**, select **Active Sites**, select **IT Services** from the **Active Sites** list, select **Site contents**, and then select the **Service Desk Requests** list.

3. In your browser, open a new tab and enter the following URL in the address bar: **https://aka.ms/pbiSingleInstaller**

4. This opens the **Microsoft Download Center** for **Microsoft Power BI**. Scroll down to the **Microsoft Power BI Desktop** section and select **Download.**

5. In the **Choose the download you want** window, select **PBIDesktopSetup_x64.exe** then select **Next** on the bottom of the screen. The status of the download will display on the notification bar at the bottom of the screen.

6. On the notification bar at the bottom of the screen, select **Open file** once the download of **PBIDesktopSetup_x64.exe** is complete.

7. The **Microsoft Power BI Desktop (x64) Setup** wizard will begin. On the **Welcome to the Microsoft Power BI Desktop (x64) Setup Wizard** page select your language and then select **Next.** Another **Welcome** page will appear; select **Next** on this page as well.

8. On the **Microsoft Software License Terms** page, select the check box to accept the license terms and then select **Next.**

9. On the **Destination Folder** page, accept the default location and select **Next.**

10. On the **Ready to install Microsoft Power BI Desktop (x64)** page, select **Install**.

11. On the **Completed the Microsoft Power BI Desktop Setup Wizard** page, select **Finish.** This will launch the Power BI Desktop.

12. When the **Power BI Desktop** opens, a window will appear in the middle of the screen that has three panes. The left-hand pane is a **Power BI Desktop** pane that enables you to **Get data**, view **Recent sources**, and **Open other reports**. The middle pane is a **Collaborate and share** pane in which you can select **Get started** to use Power BI. The right-hand pane provides free tutorial videos and links to **What's New**, **Forums**, **Power BI Blog**, and **Tutorials**. Feel free to review any of this information.

    When you are ready to proceed, select the **X** in the upper right-hand corner to close this window.

13. If you are already signed into Microsoft 365, then you may automatically be signed into Power BI Desktop as the same user that is signed into Microsoft 365. However, if the **Sign in** option appears in the upper-right corner of the screen, then select it now to sign in.

    Assuming you must sign in, select the **Sign in** option. On the **Enter your email address** dialog box, enter Holly@xxxxxZZZZZZ.onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the email address field and then select **Continue**.

    In the **Pick an account** window that appears (which may take a minute or so to appear), select Holly@xxxxxZZZZZZ.onmicrosoft.com. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.

14. In the **Power BI Desktop**, you want to create a new report based on the Service Desk Ticketing system you created earlier. You must begin by naming the report, so select **File** from the menu bar, select **Save as,** and enter **ServiceRequestPowerBI** in the **File name** field. By default, the file will be saved in the **Documents** folder as a Power BI file (.pbix). Select **Save**.

15. In the ribbon that appears at the top of the screen below the menu bar, select **Get data**. In the drop-down menu that appears, select **More...**

16. In the **Get Data** window that opens, type **SharePoint** in the Search box that appears above the left-hand navigation pane. In the detail pane on the right, three SharePoint options will appear. Since you used the on-premises version of SharePoint to create the Service Request Ticketing system, select **SharePoint Online List**, and then select **Connect**.

17. In the **SharePoint Online lists** window that appears, enter the following URL for the Service Request Ticketing system in the **Site URL** field: https://xxxxxZZZZZZ.sharepoint.com/sites/ITservices (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting partner). Select **OK.**

18. In the pop-up window that appears that displays the SharePoint site URL at the top and three authentication options on the left-hand navigation pane (Anonymous, Windows, and Microsoft Account), select **Microsoft Account**. A message will be displayed indicating you are not signed in. Select the **Sign in** button. In the **Pick and account** window, repeat the previous steps to sign in as **Holly**.

    The message that indicated you were not signed in will now change to indicate that you are currently signed in. Select **Connect**.

19. A **Navigator** window opens that provides a list of tables from the SharePoint data source that is used by the Service Desk Ticketing system. In the list of tables that appear in the left-hand pane, select the check box to the left of **Service Desk Requests**. The details for this table will then appear on the right side of the window. If the details for this table do not appear, select the **Refresh** icon on the top right corner of the navigator window.

    Note: If you select **Service Desk Requests** but do NOT select the check box, the details for the table will display in Preview mode on the right, and the buttons at the bottom of the screen will be disabled. Since you want the buttons enabled, you must select the check box to the left of **Service Desk Requests**.

    Important: Even though the **Load** button is highlighted by default, **do NOT select it or press Enter - in fact, do NOT select any of the buttons at the bottom of the page at this time!!** There are a couple of fields that need to be manipulated first before you load them into the Power Query editor. You will do that in the next step.

20. In the detail pane on the right side of the **Navigator** window, select the scroll bar at the bottom of the window and scroll to the right to view the data. While you will scroll past many fields that you will probably not recognize, look for the fields that are part of your SharePoint list.

    Also note that the names of some of the fields will not map to the names used in the SharePoint list. This is due to the fact that some SharePoint fields are predefined, and in SharePoint sites, you rename them to map to whatever actual value you have in the site. For example, as you scroll to the right, note that the **Title** column displays the **Issue Status** that appears in the ticketing system.

    What you will not see in the list of fields are the **Customer** and **Assign To** fields that display the users' names. Instead, you will see a **CustomerId** field and an **AssigntoId** field, both of which contain numerical values rather than the actual persons' names. This reason for this is that name fields are a special type of lookup field. The numerical values stored in these fields actually point to the record associated with the person, and each record stores more information for that person than just his or her name (even though the SharePoint list displays only the name).

    Therefore, you must instruct Power BI as to what specific information you want retrieved from the **Customer** and **Assign To** records. For the Power BI report, you only want to display each person's name, just as you do on the SharePoint list.

    You will do this in the next few steps when you use the **Power Query Editor** to select the person's name from the **Customer** and **Assign To** records.

21. Now that you understand how the Customer and Assign To fields are handled, you are ready to proceed. At the bottom of the window, select the **Transform Data** button, which opens the **Power Query Editor**. Maximize this window.

22. The **Power Query Editor** provides a great deal of functionality that enables you to transform data, clean data, create relationships between tables, and so on. For this exercise, you will use the Power Query Editor to focus on the simplest way of getting the persons' names to appear in the Customer field and the Assigned To field.

    In the **Power Query Editor**, use the scroll bar to scroll to the right until you find the column labeled **FieldValuesAsText** (this column is in the middle of a bunch of columns whose rows display the word **Record** in orange-colored font; so you can quickly scroll to the right until you come upon the orange colored Record rows and then locate the **FieldValuesAsText** column). Select the icon to the right of the **FieldValuesAsText** column name.

23. This opens a new window that shows all the columns that associated with this data type. In the top right corner of this window, select the "A thru Z" sort box that appears to the right of the Search field, and in the menu that appears, select **Name**. In the list of columns, the first check box is **(Select All Columns),** and since it is selected, all the columns below it are selected. You want to unselect this check box, which unselects all the other columns. The reason for doing this is that you only want to select the **Customer** and **Assignto** columns, which you will do in the next two steps.

24. Scroll down through the list of columns until you locate the **Assignto** column and then select its check box.

25. Then scroll down to the **Customer** column and select its check box.

26. Select **OK**.

27. Note how the **FieldValuesAsText** column is replaced with two **FieldValuesAsText**-related columns, one titled **FieldValuesAsText.Customer** and the other **FieldValuesAsText.Assignto.** The names associated with these fields are displayed for each record from the SharePoint list.

28. On the far-left end of the ribbon at the top of the **Power Query Editor**, select **Close & Apply**. In the drop-down menu that appears, select **Close & Apply**.

    An **Apply query changes** window appears that shows the progression of applying the data from the SharePoint list to the report. It will take a few seconds for the query changes to apply.

29. Once the query process completes, a **Fields** pane should appear on the far right of the screen. If the **Fields** pane is not expanded to show the actual fields, select the left pointing arrow (<) that appears above **Fields** to open the pane.

The **Fields** pane should display the fields associated with the **Service Desk Requests** list. If you only see the Search field and the table name **Service Desk Requests**, then select the down arrow that appears to the right of **Service Desk Requests** to display all the fields.

30. You will now create visualizations for your Power BI report. Power BI Desktop treats visualizations similar to how Microsoft Excel treats workbooks. Notice the Page tabs at the bottom of the desktop; these are similar to the workbook tabs used in Excel. Whereas Excel refers to each tab/workbook as a Sheet, Power Bi refers to each tab as a Page. And just as you can rename a workbook in Excel, so too can you rename a visualization in Power BI - simply right-click on a Page tab and rename it.
    There is one major difference between an Excel sheet and a Power Bi page. An Excel sheet only contains one workbook; however, a Power BI page can have multiple visualizations on the page.

    For this visualization, right-click on **Page 1** and select **Rename Page** in the menu that appears. Enter **Service Request Tickets** as the new name and press Enter to change the page name.

31. The **Visualizations** pane (which appears to the left of the **Fields** pane) includes a series of icons that represent the different types of visualizations that you can create. If you do not select an icon from the **Visualizations** pane, the default visualization type will be applied, which is a **Table**.

    The first visualization that you create will use the default **Table** visualization. While you do not have to select an icon for the Table visualization, it is recommended that you do so to see how it will appear in the report canvas. When you hover your mouse over each icon, the visualization type is displayed. Select the **Table** icon (fifth row, second from the left; hover your mouse over it to verify this is the correct icon before selecting it).

32. Now that you have selected the type of visualization that you want to create, you must select the fields that you want displayed in the visualization. As you select each field, note how they appear in the table visualization in the report canvas. Do not worry about the order in which they appear; you will change the order once all the fields are selected.

    In the **Fields** pane, select the check boxes next to the following fields (note – actual field names are not always the same as the field name displayed in the SharePoint list):

    - Created – select the **Created** check box
    - Customer – select the **FieldValuesAsText.Customer** check box
    - Assigned To – select the **FieldValuesAsText.Assignto** check box
    - Issue Title - select the **issueTitle** check box
    - Location – select the **Location** check box
    - Issue Status – select the **Title** check box

33. You can change the size of the table visualization in the report canvas by selecting the bottom right corner of the table and dragging it diagonally down to the right. Keep in mind that you will be adding a second visualization to this page, so leave enough room in the report canvas to add another visualization.

34. The columns will appear in the visualization in the same order in which they were selected. In the prior step, the column names were simply listed in the sequence in which they appeared in the list; this made it easier to select them as you scrolled down through the list.

    However, now you want to rearrange the columns to appear in the order that you want. In the **Visualizations** pane, below the six rows of icons is a row of three tabs that are represented by icons: **Fields**, **Format**, and **Analytics.** The **Fields** tab, which is selected by default, displays the list of fields in the order in which they will appear in the table. To move a field to the left, select the field and drag and drop the field up in the list until it appears where you want. To move a field to the right, select the field and drag and drop it down in the list until it's in the correct location.

    Note: Alternatively, you can select the down arrow in the field, and in the menu that appears, select **Move**, and then select **Up** or **Down**. Since you would have to repeat this process multiple times to move a field multiple positions to the left or right, it is much simpler to just drag and drop the field in the list of **Values**.

    Take this opportunity to arrange the columns in whatever order you want.

35. Next, you want to rename the columns so that they map to the user-friendly column names used in the SharePoint list rather than their database field names. To rename a field, under the **Fields** tab in the **Visualizations** pane, select the drop-down arrow for the field, select **Rename for this visual** in the menu that appears, and then enter the new name and press Enter.

    Change the names of the following fields:

    - FieldValuesAsText.Customer – rename to **Customer**
    - FieldValuesAsText.Assignto – rename to **Assigned To**
    - issueTitle – rename to **Issue Title**
    - Title – rename to **Issue Status**

      This completes the **Table** visualization.

36. You will now create a second visualization for this page; this will be a **Stacked Column Chart** visualization that displays the total count of service tickets by **Location** and **Issue Status**.

    You will create this visualization on the same page as the **Table** visualization. To do so, you must ensure that the **Table** visualization you just created is NOT selected. Move your mouse to a white space on the report canvas and left-click on the white space where you want your new visualization to appear.

    Important: If you select a new visualization while the current visualization is selected, the current visualization will be deleted. If this occurs, press **Ctrl-Z** to undo the deletion.

37. In the **Visualizations** pane, select the **Stacked column chart** icon (top row, second from left; verify by hovering your mouse over the icon to see its name). Note the visualization of the chart that appears on the report canvas. Increase the size of the chart by dragging its bottom-right corner down diagonally.

38. You now want to define the chart's horizontal axis. In the **Fields** pane, select the **Location** field, and holding your left mouse button down, drag the field into the **Add data fields here** box for the **Axis** option in the **Visualizations** pane.

39. In the **Fields** pane, select the **Title** field (this is the Issue Status in the SharePoint list) and drag it into the **Add data fields here** box for the **Legend** box in the **Visualizations** pane.

40. In the **Fields** pane, select the **Title** field again and drag it into the **Add data fields here** box for the **Value** box in the **Visualizations** pane.

41. Since the Title field is referred to as the Issue Status in the SharePoint list, you want to rename it here to reflect this name in the chart.

    - In the **Legend** field, select the **drop-down arrow** next to **Title**, and in the menu, select **Rename for this visual**. Enter **Issue Status** as the new name of the **Legend**.
    - In the **Value** field, select the **drop-down arrow** next to **Count of Title**, and in the menu, select **Rename for this visual**. Enter **Count of Issue Status** as the new name of the **Value**.

42. To change formatting of the chart, ensure the chart is selected. If the chart is not already selected, click your mouse inside the area of where the chart had previously appeared; this will display the chart outline.

43. In the **Visualizations** pane, select the **Format** tab (its icon appears to the right of the Values icon).

44. In the **Format** tab, all the objects that you can format (General, Legend, X axis, Y axis, and so on) appear below the **Search** field. Select the **down-arrow** key next to **Legend.** This displays all the values that can be formatted for the **Legend.**

45. The first Legend object is **Position**. In the **Position** field, select the drop-down arrow and select **Right center**. Note how the legend now appears centered on the right side of the chart.

46. Select the **up-arrow** key next to the word **Legend** to collapse the Legend options.

47. On the **Data labels** option, the toggle button is currently set to **Off**. Select this toggle button to turn it **On.**

48. Scroll down past the **Data labels** option and locate **Title**, then select its **down-arrow** to display the **Title** options. Within the **Title** object, update the following options:

    - Enter **Ticket Count by Location and Issue Status** in the **Title text** field.

- Scroll down to the **Font color** option and select the color of your choice for the Title.

- Scroll down to the **Alignment** option. The **Left**-aligned icon is currently selected. Change this by selecting the **Center**-aligned icon.

- Note the changes to the Title – the Title text, the color, and the alignment.

49. Scroll back up in the list of options until you get back to **Title**. Select the **up-arrow** to collapse the **Title** options.

50. From the **Title** option, scroll down and locate the **Border** option and then update the following settings:

- The toggle button is currently set to **Off**. Select this toggle button to turn it **On**, which will display a border around the chart.

- Select the down-arrow next to **Border** to see the available border options. In the **Color** option, change the color of the border to the color of your choice.

This completes the stacked chart visualization.

51. Now that both visualizations are complete, note the data displayed for each. Both visualizations are based on ALL the records stored in the **Service Desk Requests** SharePoint List. Now let's see what happens when you create data filters that filter the records viewed in each visualization. For example, if you created a filter for a specific customer, only the records for that customer would be processed by each visualization (as opposed to all customers that would be displayed by default).

By creating a filter for the page, all visualizations on the page will be updated based on that filter. On the **Filters** pane, notice there are two options: **Filters on this page** and **Filters on all pages**. Each filter option enables you to add data fields that will apply to that option. For this lab, you are going to update the **Filters on this page** option by creating two filters – one by **Customer** and the other by **Issue Status**.

In the **Fields** pane, select **FieldValuesAsText.Customer** and drag it into the **Add data fields here** box that's under the **Filters on this page** option. This filter will show you the list of customers from the records in the SharePoint list, and it will display the number of records for each customer. If there are tickets that have no customer assigned to it, the filter option will appear as a number until a person is assigned. If you select one or more of these customers, the visualizations will only reflect the records for those customers. By default, all customers are displayed in the visualizations.

52. Now add a second filter based on the Issue Status of each service request ticket. Scroll down in the **Filters** pane until you are past the list of customers. Note that another **Add data fields here** box now appears. From the **Fields** pane, locate the item labeled **Title** (this is the **Issue Status** in the SharePoint list) and drag it into the **Add data fields here** box that's under the **Filters on this page.**

53. Now test out the filters that you just defined for this page. Select **Megan Bowen** in the **Customer** filter. In the Table visualization, note how it eliminated all service request tickets except for those with **Megan Bowen** as the **Customer**. Also note the change to the stacked chart visualization since it only applies to the tickets in which Megan is the Customer. For the stacked chart visualization, it still counts the records with any of the three issue statuses.

54. Now let's implement the second filter. In the **Title** (Issue Status) filter, select **Active.** Note how the number of records changed in the **Table** visualization; these are the service request tickets with Megan as the Customer and an Active status. Note also how the stacked chart only includes the records with Megan as the Customer and an Active status.

55. Now change the value(s) selected in the **Title** (Issue Status) filter to see how the visualizations change as the values selected change. Unselect **Active** and select **New**. Note the change to the list. Then unselect **New** and select **Resolved**. Note the changes to both visualizations as you change the selected filter value. Next select both **New** and **Resolved** and note the change.

56. Set each filter back to display all the records by selecting **Select all** for each filter; this clears all the check boxes for each filter.

57. Save your work by selecting the **Save** icon in the top left corner of the screen.

58. To publish your Power BI report, select Home on the menu bar, and then on the ribbon, select **Publish.**

59. From the **Publish to Power BI** window that appears, select **My workspace** and then press **Select**.

60. Once published, a green check mark will appear next to the word **Success!** Select **Got it** to close the window.

61. Close the Power BI Desktop by selecting **X** icon in the top right corner of the screen.

16.0.2 Task 2 - Create a Dashboard and view from Mobile device

Adatum's IT Consultant has explained to Holly that once she has created a report that contains one or more visualizations, she can then create a dashboard based on that report. In fact, she could create a dashboard from a report, from scratch, from a dataset, or by duplicating an existing dashboard. Since pinning visualizations from a report that's already been built onto a dashboard is the quickest and easiest way to create a dashboard, Holly has decided that this is the route she is going to take. For her pilot project, Holly has decided to create a dashboard from the report that she created in the prior task.

Dashboards can only be created in Power BI Online because they are a feature of the Power BI service; they cannot be created in Power BI Desktop. Unlike Power BI reports, which are based on a single dataset and can created in both the Power BI Service and Power BI Desktop, dashboards can be based on one or more datasets and are a feature of just the Power BI Service.

Note: At the end of this task are steps on how to use your mobile device to view the dashboard that you created. These steps are strictly optional.

1. After having completed the prior task, you should still be logged into LON-DC1 as the **Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. In your Edge browser, open a new tab and then enter the following URL in the address bar: **https://powerbi.microsoft.com**

3. This opens the **Microsoft Power BI service**, which is required to create a dashboard. On the right-hand side of the top row, select **Sign in**. In the **Pick an account** window, select Holly's account (**holly@xxxxxZZZZZ.onmicrosoft.com** (where xxxxxZZZZZ is the tenant prefix provided by your lab hosting provider). In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**. In the **Stay signed in?** window, select **Yes**.

4. In the left-hand navigation pane, select **My workspace.**

   Note: Since Holly is the same user who created the report that she now wants to pin to a dashboard, she should select **My workspace** (this will show just her work). However, if she was going to use a report created by another Adatum user, she would select **Workspaces** and then select **Adatum Corporation** (or if she was collaborating with a user from another organization that had shared a report with her, she would select that organization instead).

5. At the top of the **My workspace** page you will see 3 tabs: **All**, **Content**, and **Datasets + dataflows**. On the **All** tab, which is displayed by default, two **ServiceRequestPowerBI** objects are displayed - one is the report that you just published and the other is a dataset (see the **Type** column). Select the **ServiceRequestPowerBI** report.

6. In the top-right corner of each visualization are several icons. Depending on the visualization size, they may not appear until you hover your mouse over the top right of the visualization (the icons may also appear on the bottom right corner if the visualization is flush with the top of the screen). Hover your mouse over the top right of the **Table** visualization and the four icons will appear. Then hover your mouse over each icon to display the tool tip for each.

   For the **Table** visualization, select the **Pin visual** icon.

7. In the **Pin to dashboard** window, select **New dashboard,** enter **ServiceRequestDashboard** in the **Dashboard name** field, then select **Pin**.

8. A **Pinned to dashboard** pop-up window will appear that allows you to create a phone view that will optimize your dashboard for phone views. For now, select **Go to dashboard**.

   Note: If you do not select anything when this pop-up window appears, it will close after a few seconds and you will remain in the report window. If this happens to you (for example, you were reading this instruction and the pop-up window suddenly closed), then in the left-hand navigation pane, select **My workspace**, and then under the **All** tab select the **ServiceRequestDashboard** you just created.

9. On your Dashboard page, notice at the top of the page how you can ask a question about your data. Select **Ask a question about your data**, which displays a Q&A screen with several predefined questions related to the data displayed in your dashboard. Select one of the available questions. If you enter your own question, Power BI will show a list of available questions that map to the text that you are typing.

   If you select **Exit Q&A** on the top left corner of the screen, you will return to the dashboard. However, in the next step you want to pin the stacked column visualization to the dashboard, so you need to return to the report view.

   The top row of the page displays the **My workspace > ServiceRequestDashboard > Q&A** navigation thread. Select the **My workspace** portion of this thread.

10. In your **My workspace** page, in the **All** tab, select the **ServiceRequestPowerBI** report.

11. For the stacked column visualization, select the **Pin visual** icon. In the **Pin to dashboard** window that appears, the **Existing dashboard** option is selected by default, and the dashboard name is selected by default in the **Select existing dashboard** field. Since this is the dashboard you want to pin the visualization to, select **Pin**.

12. In the **Pin to dashboard** pop-up window, select **Go to Dashboard**. If this window disappears before you can make this selection, then in the left-hand navigation pane, select **My workspace**, in the **All** tab, select **ServiceRequestDashboard**.

13. At this point you may be wondering why you created the dashboard since you have the same information in your report. In this lab exercise, you only have one report, but a dashboard can be made up of visualizations from many different reports. A dashboard provides a one-page view of your most important metrics, from one or many reports, and provides an entry way to the underlying reports and datasets.

   Select either visualization on your dashboard and note how you are taken back to the underlying report.

14. On the left-hand navigation pane, select **My workspace**.

15. On the main screen, under the **All** tab, hover your mouse over the name of the dashboard you created. This will display several icons to the right of the dashboard name, one of which is a **star** icon. You can mark this dashboard as one of your favorites by selecting this icon. Select the **star** icon.

   `Notice that when you select the star, it changes to a solid star rather than the outlined star tha`

Select the star icon again to make it one of your favorites.

16. In the left-hand navigation pane, select **Favorites**. You should see this dashboard in your list of favorites. Select the **ServiceRequestDashboard** to open it.

17. **THE REMAINING STEPS IN THIS TASK ARE OPTIONAL.**

   If you do not perform these remaining steps, leave the Power BI service open in your browser and proceed to the next task.

18. Now that you have created your dashboard, you can view it on a mobile device if you wish. In the menu bar at the top of the dashboard, select **Edit**. In the menu that appears, select **Mobile view**.

19. If a **Phone Version** dialog box appears, select **Continue**.

20. An **Edit phone view** screen will appear that shows how the dashboard will appear on your mobile device. If you hover your mouse over each visualization, a border will appear. You can select a border and drag it to change the size of the visualizations.

21. To run the app from your mobile device, you must first download and install **Power BI** from the **App Store** or **Google Play**.

22. Once you have downloaded and installed the **Power BI** app to your phone, open the app and sign-in as **holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is tenant prefix provided by your lab hosting provider).

23. You will see the dashboard and report listed on under **Recents.**

24. The dashboard will also show up in your Favorites. Select the favorites icon on your mobile device (on the bottom of the screen for an iPhone), then select your dashboard.

25. Leave the Power BI service open in your browser and proceed to the next task.

16.0.3   Task 3: Share a Power BI Dashboard

As part of her pilot project, Holly wants to share the dashboard that she just created with Laura Atkins.

1. After having completed the prior task, you should still be logged into LON-DC1 as the **Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. You should also have the Power BI Service open in your Edge browser; if not, then open a new browser tab, enter **https://app.powerbi.com** in the address bar, and sign in as **Holly.**

3. In the **Power BI** tab in your browser, in the left-hand navigation pane, select **My Workspace.**

4. On the main screen, select the **Dashboards** tab (if necessary)**.** To the far right of the dashboard name are a series of icons that appear under the **Actions** column heading. Hover your mouse over each icon to see their tool tip.

   Select the **Share** icon.

5. In the **Share dashboard** pane that appears, under the **Share** tab, you will enter the name of the person with whom you want to share the dashboard.

   In the **Enter email addresses** field, enter **Laura**, and then in the list of Adatum users whose first name starts with Allan, select **Laura Atkins.**

6. Towards the bottom of the Share dashboard pane, review the options that are already selected with a check mark. Leave the boxes checked and select **Share**. Once the dashboard is shared, you will see a message that says **Success!! Your dashboard has been shared successfully.**

7. Switch to **LON-CL1** so that you can test whether the dashboard was successfully shared.

8. On **LON-CL1**, you should still be logged in as the **Administrator** with a password of **Pa55w.rd**.

9. Open your Edge browser and enter the following URL in the address bar: **https://app.powerbi.com**

10. In the **Sign in** window, scroll down on the page until you reach the **Sign up and get started today** pane, enter **Laura@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **Enter your work email address** field, and then select **USE IT FREE**.

11. If a **You have an account with us** window appears that indicates Laura is already using another Microsoft service, then select **Sign in** to enter your existing password. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.

12. In the **Almost there** window, leave the check box blank so that Microsoft does not share Laura's information with partners, and then select **Start**.

13. In the **Invite more people** window, scroll to the bottom and select **Skip**.

14. If the **Pick an account** window reappears, select Laura's account.

15. In the **Power BI** window, in the left-hand navigation pane, select **Shared with me.** Verify that the shared **ServiceRequestDashboard** is listed. Select the dashboard to verify that it opens and displays the report information.

Note: You would perform similar steps if you shared a report with another user; sharing within Power BI is not limited to just dashboards.

16. Leave your Edge browser open and do NOT close the Power BI Service tab.

16.0.4   Task 4: Explore the Power BI Admin Portal

Now that Holly has created a report and dashboard and shared it with another Adatum user, she wants to explore the administrative functionality within Power BI that's available in the Power BI Admin Portal.

1. Switch back to **LON-DC1**.

2. On **LON-DC1**, you should still be logged in as the **Administrator** and a password of **Pa55w.rd**; if not, then do so now.

3. In your **Edge** browser, you should still have the **Power BI Service** tab open; if not, open a new tab and enter the following URL in the address bar: **https://app.powerbi.com**

4. At the top side of the **Power BI service screen**, to the right of the **Search** field, select the **gear (Settings)** icon, and in the menu that appears, select **Admin portal**.

5. In the navigation pane for the **Power BI Admin portal**, select **Tenant Settings**. Under **Workspace settings,** select **Create workspaces (new workspace experience)**. Under this option it should display a message that says: **Unapplied changes**. This indicates that you have settings that have not been applied towards creating new workspaces.

   Select **Unapplied changes**. There are two settings on this page that you need to be aware of. The first is an Enabled/Disabled option that controls whether users in the organization can create app workspaces. Verify this setting is **Enabled**; if not, then select the toggle so that it's Enabled. The second option indicates how you want to apply the permission to create workspaces. If **The entire organization** option is not selected, then select it now.

6. Select **Apply**. Note the message indicating that it may take 15 minutes to apply these permission changes. However, proceed ahead and hopefully you will not have to wait this time to create a new workspace.

7. Note that the Power BI Service's navigation pane and the Admin portal's navigation pane both have a **Workspace** option. However, you can only create a workspace through the Power BI Service. You can add members to a workspace using either one, but you can only create a workspace through the Power BI Service.

   In the left-hand navigation pane for the **Power BI Service**, select **Workspaces**.

8. If a **You have unapplied changes** window appears, select **Apply all**.

9. In the **Workspaces** pane that opens, select the **Create a workspace** button at the bottom of the pane.

10. In the **Create a workspace** pane that opens, enter **Test Workspace** as the workspace name and then select **Save**.

11. You just created the workspace using the Power BI Service, so now let's see what workspace functionality is available in the Power BI Admin Portal.

    After you saved the workspace in the prior step, it took you to the workspaces page for the workspace that you just created (the **Welcome to the Test Workspace** page). You can return back to the **Admin portal** by selecting the back arrow (to the left of the address bar) twice, or by selecting the **gear (Settings)** icon and then selecting **Admin portal**.

12. Select **Workspaces i**n the **Admin portal's** navigation pane. **Test Workspace** should appear in the list of Workspaces. Select the **Test Workspace** name, which displays a check mark to the left of the name. In the menu bar that appears above the list, select **Details**. Review the information in the **Details pane** and then close it.

13. With the **Test Workspace** still selected, select **Edit** on the menu bar. In the **Edit workspace pane**, note how you can change the workspace name and description even though you could not add a workspace using the **Power BI Admin portal**. Close the **Edit workspace pane**.

14. With the **Test Workspace** still selected, select **Access** on the menu bar. In the **Access pane**, note how you can add members to this workspace (you can do this through the **Workspaces** option in the **Power BI Service** as well). In the Enter email addresses field, enter **Patti**. In the list of users whose first name starts with Patti, select **Patti Fernandez** and then select **Add**. As you can see in the bottom portion of the pane, Patti now has **Member** permissions to this workspace. Close the **Access pane**.

15. In the **Admin portal's** navigation pane, select **Tenant settings**. Scroll down through the **Settings** page and review the settings that are available.

16. Scroll to the **Custom Branding** section at the very bottom of the **Settings** page. The **Theme Color** field controls the color scheme for the **Power BI Service**, which by default is set to black and gold. Go ahead and change the color to see the color scheme change in the Power BI Service.

    To change the color scheme, select the **black box** in the **Theme color** field to display the color palette. Drag the circle in the slider bar to the right until you locate a color combination that you like. Locate the circle that appears in the large colored square. Select this circle and drag it around the gradient colors.

Note how the hex color codes change as you drag the circle. Once you find a color that you prefer, release your left-mouse button and select anywhere on the screen outside the color box to change the **Theme color**. Then scroll to the bottom of the page and select **Publish**.

17. In the **Publish your changes?** dialog box that appears, select **Publish**.

18. In the **Published!** dialog box, select **OK**.

19. Select the **Refesh** icon that appears on the address bar and note the color scheme change when the **Power BI Service** page refreshes itself. You can repeat this process until you find a color combination that you prefer.

20. Select any of the other options in the **Admin portal's** navigation pane that are of interest to you.

21. When you are done, close the **Power BI** tab in your Edge browser.

17 End of Lab 3

18 Module 4 - Lab 3 - Exercise 1 - Review Key Features of Exchange Online

Holly Dickson is Adatum's Enterprise Administrator. She has recently deployed Microsoft 365 in a virtualized lab environment. Now that she has a tenant account set up and has been assigned to the Global Administrator role, she has been asked to review the key administrative functions within Exchange Online, SharePoint Online, and Teams so that she becomes familiar with their functionality and can offer guidance to her IT team on how they can be used throughout Adatum.

With regard to Microsoft Exchange, Adatum's CTO has requested that Holly review some of the basic administrative functions in Exchange Online related to mail flow and recipient management. Since the Global Administrator role includes the Exchange Administrator role, Holly can perform all Exchange-related tasks.

18.0.1 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.

1. At the end of the previous lab, you were on LON-CL1, where you took on the role of Laura Atkins and installed Microsoft 365 Apps for enterprise. For this lab exercise, you must switch back to LON-DC1, where you will resume your pilot project in the role of Holly Dickson.

    Switch to **LON-DC1**, where you should still be logged in as the **Administrator** with a password of **Pa55w.rd**; if not, then do so now.

2. You should still have an Edge browser session and the Microsoft 365 admin center open from the prior lab. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix 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** in a new tab. This is the Exchange admin center for Microsoft 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 across the top of the page - mailboxes, groups, resources, and so on). 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 the mailboxes for Holly Dickson and Laura Atkins that were created when you added their Microsoft 365 user accounts in the prior lab.

    Select the mailbox for **Joni Sherman** by clicking on her **DISPLAY NAME.** This will open the **User Mailbox** window with Joni's data prefilled. By default, the window displays the **Mailbox** tab (the tabs appear at the top under Joni's name).

6. At the bottom of the **Mailbox** tab, Under more **More options** select **Custom attributes**.

7. 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.

8. In addition to the **Mailbox** tab, there is the **Account** tab which combined includes several other sections 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 additional 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.

9. Select **mailbox delegation.** This enables the admin to assign a user to this mailbox's Send As, Send on Behalf permissions, or Read and manage. This option is commonly used if you want another user to be able to send messages from this mailbox.

10. While in the **mailbox delegation** window and select **Edit** to the right of **Read and manage**

11. In the *Manage Mailbox deligation* window, select **+ Add permissions**. In the search bar type in **Holly Dickson** and select **Holly Dickson** from the list of user accounts, select the **Save** button. Then select **Close** then **cancel** twice

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

12. On Joni Sherman's **Mailbox** window, select the **X** in the top right hand of the pane.

13. Leave your browser and all the tabs open for the next task.

18.0.2   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 a Microsoft 365 group.

1. Your browser should still be open to the **Exchange admin center** from the prior task, and 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 already see the **Inside Sales** group that you created in Lab 2. This is a Microsoft 365 group whose email address is associated with the custom, on-premises domain (@xxxUP-Nxxx.xxxCustomDomainxxx.xxx). In the following steps, you will create a Distribution list group and a Microsoft 365 group whose email addresses will be in Microsoft 365 (@xxxxxZZZZZZ.onmicrosoft.com).

2. Select **Add a group** button under the Microsoft 365 tab.

3. In the **Choose a group type** window that appears, choose **Distribution** and click **Next**.

4. In the **Set up the Basics** tab, add the group name of **Sales Department** next to **Name** and leave description blank and select **Next**.

5. In the **Edit settings** tab Enter the following then click **Next**:

   - Email Address: Type in **SalesDept**. In the domain field to the right of it, select the drop-down arrow and select **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

   - Joining the Group: Select **Owner Approval** This allows the owner to control who can join the group.

- Leaving the Group: Select **Closed** This allows the owner to control who can leave the group. Together with Joining the group you can control who joins or leaves your distribution. However if you need less administration leaving open for either is an option.

6. In the next section select **Create group** and click **Close**

7. Wait until you see your group name under the **Distribution list** tab. If you don't see it, refresh every 5 minutes.

8. Once you see your new group, **Sales Department**, click on the group name and click on the **Members** tab.

9. Click on **View and manage 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 the back arrow.

10. Click on **View and manage members** now.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 back arrow.

11. Verify the changes are made and the click on the **X** in the top right hand corner.

12. Select the **Add a group** button.

13. In the **Choose a group** window that appears, choose **Dynamic distrabution** and select **Next** enter the following information:

    - Group name: **Dynamics CRM Project Team**

    - Description: **Adatum users working on the Microsoft Dynamics CRM project.**

14. In the **Assign users** Enter the folling inofrmation then click on **Next**:

    - Owners: **Holly Dickson**

    - Members: Ensure **All recipient types** is selected

15. Under **Edit settings** Enter the folling inofrmation then click on **Next**:

    - 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 **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)

16. Select **Create Group** and then select **Close**.

17. Go to the **Dynamic distribution list** and click directly on **Dynamic CRM Project Team**.

18. In the **Dynamics CRM Project Team** window, the **Members**. Under **Owners**, select the **View all and manage owners**, and in the **Add Owners** window, select **Nestor Wilke**, select the **add** button, and then select back arrow.

19. Ensure all changes were made then close out of the **Dynamics CRM Project Team** window.

18.0.3 Task 3 - Upgrade Distribution Lists

Organizations have typically relied on distribution groups in Exchange to communicate and collaborate with groups of people both inside and outside the company. However, Microsoft 365 Groups offer a more powerful solution for collaboration, and Adatum's CTO wants to take advantage of this feature. He has asked you to upgrade the company's Sales Department distribution list to a Microsoft 365 group so that Adatum's Sales staff can choose the people they want to collaborate with and easily set up a collection of resources for those people to share.

1. In the **Exchange admin center**, you should still be displaying **recipients** from the left-hand navigation pane, and you should still be displaying the **groups** tab.

2. Select the circle to the left of the **Sales Department** distribution list and when you see a check mark select the three horizontal ellipses and select **Upgrade distribution group**.

3. A **Ready to upgrade** pop up will appear. Select **Upgrade**. This may take up to 5 minutes for it to show up under your **Microsoft 365** tab

4. If the **Sales Department** group still displays as a **Distribution list**, then select the **Refresh** icon in the menu bar above the list; the Sales Department group will now display as a **Microsoft 365** group.

18.0.4 Task 4 - Configure a Group Naming Policy

A group naming policy enables organizations to standardize and manage the names of distribution groups created by its users. You can require that a specific prefix and suffix be added to the name for a distribution group at the time it's created, and you can also block specific words from being used. This helps organizations minimize the use of inappropriate words in group names.

Adatum's CTO wants Holly to implement a standard naming policy throughout the organization based on the following format: **{Department}{Group Name}{City}**

1. In the **Exchange admin center**, you should still be displaying the list of groups. In the menu bar that appears over the list of groups, select **Configure group naming policy.**

2. In the **Edit group naming policy** window that appears, you can select a prefix and a suffix.

   In the **For the prefix, apply the following sequence:** field, select the drop-down arrow and select **Attribute** aned to the right in the **select one** field select **Department**.

3. In the **AND** field, select the drop-down arrow and select **Text**. In the **Enter text** field, enter **Group**.

4. Select the **Add suffix** button below the **AND** field.

5. In the field that appears, select the drop-down arrow and select **Attribute**. Select the drop-down arrow, select **City**.

6. Review the **Preview policy** example that is based on the parameters you selected. If any need to be fixed, select the correct values now. When everything looks OK, select the **Save** button at the bottom of the window and close out of the pane.

18.0.5 Task 5 – 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. In the **Exchange admin center**, you should still be displaying **recipients** from the left-hand navigation pane. In this select **resources.**

2. In the menu bar, select the **Add a resource** sign and then in the new window, select **Room**.

   Note: This selection is designed for administrators to set up a meeting location for booking purposes. When scheduling meetings, you will be able to select the room from the Global Address List (GAL).

3. In the **Fill in the basic info** 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 **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)
   - Capacity: **15**
   - Location: The room is in Building 5, Room 2011, so enter **5/2011**
   - Phone: **425-555-2011**

4. Select **Next** and then select **Next** for the resource address section.

5. In the **Booking options** window select the **Allow scheduling only during working hours** check box.

6. In the **Booking delegates** type in **Holly Dickson** and **Nestor Wilke**.

   Note: This option allows a user to filter booking requests.

7. Ensure the box next to **Automatically decline meetings outside of limits below** is selected or you won't be able to input the following information.

8. In the **Booking window (days)** field, input **60** days.

   Note: 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, input **120** hours (this is five days, or one work week).

10. Select **Next** then review the resource information. Click on **Create** and wait for the resouce to be created. When it's finished, you'll see a **Done** button appear. Click **Done** and you have successfully created a new room mailbox.

18.0.6 Task 6 – 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. In the **Exchange admin center**, you should still be displaying **recipients** from the left-hand navigation pane. Select **contacts.**

2. In the menu bar that appears over the list of contacts, select **Add a contact** and in the menu that appears, in the first drop down menu 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: **Hai**
   - Last Name: **Chu**
   - Display Name: tab into the field and **Hai Chu** is automatically displayed
   - External Email Address: Hai@fabrikam.com

4. Select **Add** and then select **close** once the changes are successfully saved. Hai should now appear in the list of contacts as a **Mail contact**. If not, refresh your menu and in a minute or so you should see Hai Chu.

5. On the menu bar above the contacts list, select the **Add a contact** sign to add another contact. In the new window in the first drop-down menu, select **Mail user.** (should be selected by default)

   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: **Bill**
   - Last Name: **Norman**
   - Display Name: tab into the field and **Bill Norman** is automatically displayed
   - External email address: Bill@fabrikam.com
   - Alais: Bill
   - User ID: **Bill** (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 **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)
   - New password: **Pa55w.rd**
   - Confirm Password: **Pa55w.rd**

7. Select **Add** and then select **Close** once the changes are successfully saved. Bill Norman should now appear in the list of contacts as a **Mail user**. If not, refresh your menu and in a minute or so you should see Bill Norman.

8. Leave the Exchange admin center tab open and proceed to the next task.

18.0.7 Task 7 – Configure Messaging Protection

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.

Note: In these next three tasks you will configure malware, connection, and spam filters, respectively. These filters were previously configured in the Exchange admin center; however, starting December 1, 2020, that functionality has been moved to the Security and Compliance Center, which is where you will go to create these filters.

1. On LON-DC1, select the **Microsoft 365 admin center** tab in your Edge browser, and then in the left-hand navigation pane under **Admin centers**, select **Security**.

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

3. In the **Home > Policy** window, under the **Policies** section, select the **Anti-malware** tile.

4. In the **Home > Policy > Anti-malware** window, select the **Default** filter.

5. In the **Default** filter pane that appears, select the **Edit policy** button. This will open the **Edit a anti-malware policy** window for the **Default** policy. This window will present a variety of options on how your environment will respond, what it will respond to, and how it identifies key recipients.

6. The **Name your policy** tab in the left-navigation pane is displayed by default. Since the policy is already named, select the **Malware detection response** tab.

7. In the **Malware detection response** tab, select the **Yes and use the default notification text** option.

   Note: You will select **Save** once you have finished updating the policy, so do not select the **Save** button at this time.

8. Select the **Common attachment types filter** tab, select the **On – Email with filtered file attachment types will trigger the malware detection response (recommended)** option.

9. Select the **Notifications** tab and under the **Administrator notifications** section, select the **Notify administrator about undelivered messages from internal senders** check box.

   In the **Administrator email address** field that appears below this option, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

10. Under the **Administrator notifications** section, select the **Notify administrator about undelivered messages from external senders** check box.

    In the **Administrator email address** field that appears below this option, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

11. You have finished updating this **Default** anti-malware policy, so select **Save**.

12. On the **Security & Compliance** dialog box that appears asking whether you want to continue updating your organization settings, select **Yes**.

    Note: It may take a couple of minutes for the organization settings to get updated.

13. Leave your Edge browser open to the **Office 365 Security & Compliance** center for the next task.

18.0.8 Task 8 – Manage Connection Filters

Holly has been contacted by Adatum's CTO. He is upset that he keeps finding email from friends and business associates in his junk email folder, and he's even had email blocked entirely by a spam filter. He has asked Holly to address this problem by making sure that email sent from people who are trusted do not get blocked.

Holly has investigated the situation and has found that in Microsoft 365, you can create a connection filter policy that defines a list of IP addresses that you trust. This is known as an Allow list, or Safe Sender list. You can also create a Blocked senders list, which is a list of IP addresses (typically from known spammers) that you never want to receive email messages from.

1. In the **Office 365 Security & Compliance** center, you should still be displaying the **Home > Policy > Anti-malware** window. In this thread at the top of the page, select **Policy**.

2. In the **Home > Policy** window, under the **Policies** section, select the **Anti-spam** tile.

3. The **Home > Policy > Mail filtering** window displays a list of default **Anti-spam settings** that control how messages are handled by Microsoft 365 anti-spam policies.

   Select the drop-down arrow to the left of the **Connection filter policy (always ON)** filter. This displays the current settings for this default connection filter. Select the **Edit policy** button.

4. In the **Connection filter policy** pane that appears, the **Connection filtering** section displays options regarding which IP Addresses will be allowed to send messages to your environment and what IP addresses will be blocked from sending messages.

   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. It typically takes up to 1 hour to replicate the change within the system. For this lab, simply review the fact that you can create allowed and blocked lists of IP addresses.

5. At the bottom of the **Connection filtering** section, select the **Turn on safe list** check box. 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 they are never mistakenly marked as spam.

6. Select **Save** to save this filter, and then select **OK** once the changes are successfully saved.

7. Leave your Edge browser open to the **Office 365 Security & Compliance** center for the next task.

18.0.9 Task 9 – Manage Spam Filters

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 Global Admin, 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 Security and Compliance 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. In the **Office 365 Security & Compliance** center, you should still be displaying the **Home > Policy > Mail filtering** window after having completed the prior task.

   Select the drop-down arrow to the left of the **Default spam filter policy (always ON)** filter. This displays the current settings for this default spam filter. Take a moment and review the policy settings that are available in this filter, and then select the **Edit policy** button.

2. In the **Default spam filter policy (always ON)** pane that appears, select the drop-down arrow to the right of the **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.

3. In the **spam and bulk actions** section, make the following selections:

   - Spam: **Move message to Junk Email folder**

   - High confidence spam: **Prepend subject line with text**

   - Phishing email: **Quarantine message**

   - High confidence phishing email: **Quarantine message**

   - Bulk email: **Move message to Junk Email folder**

- Select the threshold: **5**

- Quarantine (retain spam for days): **10**

- Prepend subject line with this text: enter **WARNING: This message contains potential spam!**

4. Select the drop-down arrow to the right of the **International spam** section.

   Note: This section allows you to automatically tag messages as spam when they originate from countries/regions that are to be avoided or distrusted, as well as messages written in specific languages.

5. Under the **Filter email messages written in the following languages** setting, select **Edit**.

6. In the **International spam settings** pane that appears, select the **Filter email messages written in the following languages** check box.

7. You should already know the languages that you want to filter. In the **Languages** field, enter the first letter of a language that you want to filter. This will display all languages that start with that letter (as well as any languages that contain that letter within the name of the language).

   Enter a letter and then select a language with that letter in it that you want to filter. Repeat this step for a couple of languages.

8. Once you have finished selecting the languages you want to filter, select **Save**.

9. In the **International spam** section, under the **Filter email messages sent from the following countries or regions**, select **Edit**.

10. In the **International spam settings** pane that appears, select the **Filter email messages sent from the following countries or regions** check box.

11. You should already know the countries/regions that you want to filter. In the **Country/Region** field, enter the first letter of a country/region that you want to filter. This will display all countries/regions that start with that letter (as well as any countries/regions that contain that letter within the name of the country/region).

    Enter a letter and then select a country/region with that letter in it that you want to filter. Repeat this step for a couple of countries/regions.

12. Once you have finished selecting the countries/region you want to filter, select **Save**.

13. Select the drop-down arrow to the right of the **Spam properties** section.

    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.

14. Select the drop-down arrow to the left of **Increase spam score** and then turn **On** the following options:

    - **URL redirect to other port**

    - **URL to .biz or .info websites**

15. Select the drop-down arrow to the left of **Mark as spam** and then turn **On** the following options:

    - **Empty messages**

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

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

17. In the list of spam filters, select the drop-down arrow to the left of the **Default spam filter policy (always ON)** filter that you just edited. This displays a summary of the filter. At the bottom of the middle column of settings for this policy, the **End-user spam notifications** setting is turned **Off**. Below this option, select **Configure end-user spam notifications**.

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

19. Select **Save**. In the list of settings for this policy, note the **End-user spam notifications** setting is now turned **On** and the **Send end-user spam notifications every (days)** setting is set to **5**.

20. In your Edge browser, close the **Security & Compliance** center tab, but leave all other tabs open.

18.0.10 Task 10 – Manage Mail Flow Rules

After Holly reviewed the messaging environment at Adatum Corporation, she realized that she could provide a more efficient and secure environment if she created a set of mail flow rules that identify and take action on messages that are in-transit through her Exchange Online organization, as opposed to simply waiting until the messages are delivered to mailboxes before being acted upon by Inbox rules in Outlook and Outlook on the web.

Holly has discovered that mail flow rules contain a richer set of conditions, exceptions, and actions, all of which will provide her with the flexibility to implement many types of messaging policies for Adatum. She is eager to put this to the test regarding a significant issue currently affecting Adatum's messaging environment - users who send extremely large email messages. She has decided that her first task will be to create a mail flow rule that restricts email size.

1. On LON-DC1, select the **Exchange admin center** tab in your Edge browser, and then in the left-hand navigation pane select **mail flow**.

2. In the list of mail flow tabs across the top of the page, **rules** is already selected by default since it's the first tab.

   Note: In this section you will be presented with a variety of options to protect against emails being sent from Adatum that have sensitive information, as well as creating custom rules to prevent or track messaging-related issues from recipients in your environment. For the purposes of this lab, you will only update the email size restriction rule.

3. In the menu bar that appears over the list of mail flow rules, select the **plus (+)** sign, and in the menu that appears, select **Filter messages by size.**

4. In the **new rule** window that appears, enter the following information:

   - Name: **Email size restriction**

   - Apply this rule if: select **The message size is greater than or equal to...**

     – To the right of this drop-down field, select **Enter text**.

     – In the **specify size (KB)** window that appears, enter **1024** and then select **OK**.

   - Do the following: hover your mouse over **Block the message...**, and then in the drop-down menu that appears, select **Reject the message and include an explanation**.

     – To the right of this drop-down field, select **Enter text**.

     – In the **specify rejection reason** window, enter the following text: **Your message exceeds the size limit. Please adjust the message size or compress the email content and send it as a zipped file.**

     – Select **OK.**

   - Under **Choose a mode for this rule**, select **Enforce.**

5. Select **Save**.

6. Leave your Edge browser open as well as all the tabs.

18.0.11 Task 11 – Validate Accepted Domains

A domain that's added to an organization's on-premises environment is called an accepted, or custom domain. You can create mailboxes with accepted domains to receive and send email. In Lab 1, you created a domain for Adatum Corporation based on the unique UPN name assigned to your tenant and the custom domain name provided by your lab hosting provider (in this case, xxxUPNxxx.xxxCustomDomainxxx.xxx, where xxxUPNxxx is your unique UPN Name and xxxCustomDomainxxx.xxx is the domain created by your lab hosting provider).

In this task, you will use the Exchange Admin Center to view the accepted domain that you previously created and configure its domain type. Each domain can be changed to either authoritative (which accepts all inbound or outbound mail) or internal relay (which only accepts internal email). By default, all domains should be set to authoritative. You want to ensure that your custom domain's type is set to authoritative.

1. In the **Exchange admin center**, you should still be displaying **mail flow** from the left-hand navigation pane. In this list of mail flow tabs across the top of the screen, select **accepted domains.**

2. In the list of accepted domains, you should see Adatum's two domains – its custom on-premises domain (xxxUPNxxx.xxxCustomDomainxxx.xxx) that you added in Lab 1, and its Microsoft 365 cloud domain (xxxxxZZZZZZ.onmicrosoft.com).

3. You can see from this display that the domain type for each domain is already set to **Authoritative,** so you don't need to make any changes here.

4. However, let's assume that you set the domain type to **Internal Relay** when you initially created the custom **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain. If you wanted to change it now to **Authoritative,** you would perform the following steps (you can perform the first step to see the window and the corresponding options, but the domain is already set to Authoritative, so you can't actually make this change):

   - Select this domain in the list, and then select the **pencil (edit)** icon on the menu bar.

   - In the window for this domain, under **This accepted domain is:** you would select the **Authoritative** option and then select **Save**. However, since you did not make any changes, select **Cancel** to close this window.

5. This concludes the exercise on reviewing Exchange Online features. You can close the **Exchange admin center** tab in your Edge browser. This will return you to the **Microsoft 365 admin center** tab, which you will access in the next exercise.

19 Proceed to Lab 3 - Exercise 2

20 Module 4 - Lab 3 - Exercise 2 - Review Key Features of SharePoint Online

Adatum's CTO has heard a lot about Microsoft SharePoint and is interested in implementing it at Adatum. However, security is of the utmost concern to the CTO, who is concerned whether new sites created within the company can be kept secure. The CTO has tasked Holly with reviewing some of the basic administrative functions in SharePoint Online to determine whether it can meet their security requirements.

20.0.1 Task 1 – Site Management

A team site includes a group of related web pages, a default document library for files, lists for data management, and web parts that can be customized to meet your collaboration needs. Holly is excited about the possibility of using team sites in SharePoint Online to improve collaboration between team members when working on specific projects. As part of Adatum's pilot project, Holly wants to create a team site for the IT department so that IT personnel can work on projects and share information from anywhere and on any device.

1. You should still be logged into LON-DC1 as **Administrator** and password **Pa55w.rd**; if not, then do so now.

2. You should still have Microsoft Edge and the **Microsoft 365 admin center** open from the prior lab, and you should be logged in as Holly Dickson. If so, proceed to the next step; otherwise, open Edge, navigate to **https://portal.office.com/**, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix 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 **SharePoint.** This will open the SharePoint admin center.

4. In the **SharePoint admin center**, in the left-hand navigation pane, select **Sites**, and then select **Active sites.**

5. In the **Active sites** window, select the **+Create** option on the menu bar.

6. Depending on the team or company need, there are several templates that can be used when creating a new site. For the purposes of this lab, in the **Create a site** window, select the **Team site** tile.

7. In the **Get a team site connected to Microsoft 365 Groups** window, enter the following information.

   - Site name: **IT Services**

- Group email address: this is the alias for the group email address. As you typed in **IT Services** in the **Site name** field, the same text automatically prefilled in this field, although the blank space was removed so that it appears as one word. Do not change this default value.

- Group owner: type **Diego**, and in the window that appears displaying the users whose first name starts with Diego, select **Diego Siciliani**.

- Select a language: Leave this as **English**

- Select **Advanced settings** to expand this section and then enter the following information:

  - Privacy settings: Given the confidential nature of much of the IT department's information, select **Private – only members can access this site**

  - Time zone: since this group is in Adatum's Redmond, WA location, select **Pacific Time (US and Canada)**

  - Site Description: **Team site for the IT department**

8. Select **Next**.

9. In the **Add group members** window, in the **Add additional owners** field, enter **Holly**. As you enter Holly, a window appears listing users whose first name starts with Holly. Select **Holly Dickson**.

10. You now want to add **Patti Fernandez** and **Nestor Wilke** as members of this group.

    In the **Add members** field, enter **Patti**. As you enter Patti, a window appears listing users whose first name starts with Patti. Select **Patti Fernandez**.

11. Repeat the previous step for **Nestor Wilke**.

12. Select **Finish**. The **IT Services** site should now appear in the list of **Active sites**.

13. You're now going to test the process of deleting a team site and then restoring it. In the list of **Active sites**, select the circle to the left of the **IT Services** site name (do not select the IT Services site name, as this will open a properties window for the site).

14. In the menu bar at the top of the page, select **Delete**. If not seen click on the three horizontal elipses **…** and in the drop down menu select **Delete**.

15. In the **Delete Microsoft 365 group** window, select the **Delete the group "IT Services" and all its resources** check box and then select **Delete.** Note that the IT Services site disappears from the **Active sites** list.

16. In the left-hand navigation pane on the **SharePoint admin site**, under **Sites**, select **Deleted sites.** Note how the IT Services site that you just deleted appears in the list of deleted sites.

17. In the **Deleted sites** window, select the circle to the left of the **IT Services** site name (do not select the IT Services site name).

18. In the menu bar at the top of the page, select **Restore**.

19. In the **Restore Microsoft 365 group** window, select **Restore**. Note that the IT Services site disappears from the **Deleted sites** list.

20. In the left-hand navigation pane on the **SharePoint admin site**, under **Sites**, select **Active sites.** The IT Services site should once again appear in the **Active sites** list.

21. In the **Active sites** list, select the circle to the left of the **IT Services** site name. If you scroll to the right, you will see that the information that you previously entered for this site has been restored.

22. Remain in the SharePoint admin center for the next task.

20.0.2 Task 2 – Hierarchical Permissions

SharePoint Online uses hierarchical permissions to set authorization and access of sites. In other words, when a site is created (known as the parent site) any sites that are later created under that site (known as children sites) will, by default, inherit the main site permissions of the parent site. Since you just created a team site for IT Services, you now plan to configure site permissions to meet the IT team's security requirements.

In this task, you will create the following hierarchical permission structure for Adatum:

- When you created the IT Services team site in the prior task, you assigned Diego Siciliani as the group owner of the site, and you assigned Patti Fernandez and Nestor Wilke as group members for the site. In doing so, the default team site permission levels were assigned to Diego, Patti, and Nestor. Diego was assigned Full Control permission (as site owner), and Patti and Nestor were assigned Edit permissions (as site members). In this task, you will verify these default team site permission levels were automatically assigned to Diego, Patti, and Nestor.

- You want to assign a different set of permissions for a different group of users, so you will follow best practices by creating a group of users and assigning the group a custom permission level (as opposed to assigning custom permissions to each individual user). In this case, you will create a new **Information Technology** group, you will assign Isaiah Langer and Joni Sherman to this group, and will you assign the group Full Control permissions.

- You will then create a permission level titled **Designer**, which will be used for Adatum's web specialists who will design SharePoint sites upon request. They need to be assigned permission levels that provide complete editing and administrative capabilities. While you will not do it in this lab, you can later create a group for your web designers and assign that group this Designer permission level.

1. In the **SharePoint admin center**, you should still be displaying **Active sites**.

2. Select the **IT Services** site that you created in the prior task (do not select the circle to the left of it as you did in the prior task; instead, select the site name like you normally would).

3. In the **IT Services** window that appears, select the URL (**.../sites/ITServices**) that is displayed under **URL.**

4. A new tab will open in your Edge browser that displays the **IT Services** site. In the upper right-hand corner of the **IT Services** site (to the left of Holly Dickson's name and initials), select the **gear (Settings)** icon.

5. In the **Settings** pane that appears, select **Site permissions.**

6. In the **Permissions** pane that appears, select **Advanced permissions settings**, which opens a new **Permissions: IT Services** tab in your Edge browser.

7. In the ribbon that appears at the top of the screen, two tabs are available - a **BROWSE** tab and a **PERMISSIONS** tab, the latter of which is displayed by default.

   Select the **BROWSE** tab and note how the Permissions ribbon disappears. This also reveals the name of this page, which is **Site Settings > Permissions**.

8. Select the **PERMISSIONS** tab, which displays the Permissions ribbon. In the ribbon, under the **Check** section, select **Check Permissions.**

   Note: This option enables you to check access permissions for users and groups. In this case, you will check the permissions that were assigned to Holly Dickson. In the prior task, you assigned Holly as an owner of the IT Services site. The following steps will enable you to check what default team site permissions were assigned in this role.

9. In the **IT Services: Check Permissions** dialog box that appears, in the **User/Group** field, type **Holly**. As you type Holly, a window appears listing users whose first name starts with Holly. Select **Holly Dickson** and then select **Check now**. Since Holly is an owner of this site, this confirms that she was automatically assigned **Full Control** permissions.

10. In the **User/Group** field, select the **X** next to Holly's name to remove it from the field. In the **User/Group** field, type **Nestor**. As you type Nestor, a window appears listing users whose first name starts with Nestor. Select **Nestor Wilke** and then select **Check now.** Since Nestor is member of this site, this confirms that he was automatically assigned **Edit** permissions.

    Note: At the time of this writing, the application was displaying **None** as Nestor's permission level, which is typically attributed to someone who is not a site member. The same thing occurred when checking Diego Siciliani and Patti Fernandez. You can try checking their permissions to see if this issue has been resolved and it displays their actual permission level.

11. Repeat the prior step and check the permission for **Alex Wilber**. You will see that Alex's permission level is set to **None**, which means he does not have permission to access or update the site since he has not been assigned as a site member.

12. In the **IT Services: Check Permissions** window, select **Close.**

13. You are now back in the **Permissions: IT Services** tab in your browser. You have been asked to create a new group of users and assign them permission to access the IT Services site. In the ribbon that appears at the top of the page, under the **Grant** section, select **Create Group.**

    Best Practice: It's a best practice that you should use Groups to assign access permissions rather than assigning access to individual user accounts for two important reasons: Assigning individual users access to a site makes it difficult to track user access when the user leaves your organization, and direct permissions can override security groups permissions.

14. In the **People and Groups > Create Group** window, enter the following information:

    - Name: **Information Technology**

    - About me: **This group is used for members of the IT staff**

    - Group owner: If Holly Dickson appears as the owner, select the **X** to the right of her name to remove her, and then enter **MOD**. As you type MOD, a window appears listing users whose first name starts with MOD. Select **MOD Administrator**.

      Best Practice: When you create groups make sure the group owner is either a generic Administrator account or an Administrator group. Giving ownership of groups to individuals can cause editing issues because only the owners can make changes to groups.

    - Group Settings:
      - Who can view the membership of the group: **Group Members**
      - Who can edit the membership of the Group: **Group Owner**
      - Allow requests to join/leave this Group: **Yes**
      - Auto-accept requests: **No**
      - Send membership requests to the following e-mail address: If Holly Dickson's email appears, replace her email with the MOD Administrator's email, which is **admin@xxxxxZZZZZZ. onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)
      - Choose the permission level group members get on this site: **Full Control − Has full control**

15. Select **Create**.

16. This displays the **Information Technology** group information. The users displayed in the list are the members of this group. Since Holly Dickson created the group, she is listed as the sole member.

17. In the menu bar that appears above the user list, select the drop-down arrow that appears next to **New**, and then in the drop-down menu, select **Add users to this group.**

18. In the **Share 'IT Services'** window, the **Invite people** tab is selected in the left-hand pane by default. In the **Enter names or email addresses** field, enter **Isaiah**. As you type Isaiah, a window appears listing users whose first name starts with Isaiah. Select **Isaiah Langer**.

    Repeat this step for **Joni Sherman** (type **Joni** next to Isaiah Langer's name in the **Enter names or email addresses** field).

19. Below the personal message field, select **SHOW OPTIONS.**

20. Uncheck the **Send an email invitation** option.

21. Select **Share** to share the IT Services site with the members of this Information Technology group.

22. In the **People and Groups > Information Technology** window that appears, the members of the group (Holly, Isaiah, and Joni) should be displayed.

23. Close this **Peoples and Groups** tab in your Edge browser. This will return you to the **SharePoint admin center** and the **Active sites** list, with the **IT Services** pane open on the right-hand side.

24. In the **IT Services** window that appears, select the URL (**.../sites/ITServices**) that is displayed under **URL.**

25. A new tab will open in your Edge browser that displays the **IT Services** site.

26. In the upper right-hand corner of the **IT Services** site, select the **gear (Settings)** icon.

27. In the **Settings** pane that appears, select **Site permissions.**

28. At the bottom of the **Permissions** pane, select **Advanced permissions settings**, which opens the **Permissions: IT Services** tab for the IT Services site.

29. On the ribbon that appears at the top of the page, under the **Manage** section, select **Permission Levels**.

    Note: This option enables you to customize permission levels to better fit your organization.

30. In the **Permission Levels** window, in the menu bar at the top of the page, select **Add a Permission Level.**

31. You want to create a permission level for your team's web specialists who will be designing SharePoint sites upon request. They need to be assigned permission levels that provide complete editing and administrative capabilities. In the window that appears, enter the following information:

    - Name: **Designer**
    - About Me: **This level restricts the level of use for web designers**
    - List Permissions – select the following permission levels:
        - **Add Items**
        - **Edit Items**
        - **Delete Items**
        - **View Items**
        - **Open Items**
        - **View Versions**
    - Site Permissions – select the following permission levels:
        - **Create Subsites**
        - **Add and Customize Pages**
        - **Apply Themes and Borders**
        - **Apply Style Sheets**
        - **Browse Directories**
        - **View Pages**
        - **Enumerate Permissions**
        - **Browse User Information**
        - **Use Remote Interfaces**
        - **Use Client Integration Features**
        - **Open**

32. Scroll to the bottom of the page and select the **Create** button to save your changes.

33. The **Permission Levels** window now displays the permission level that you just added.

34. In your Edge browser session, close the **Permission Levels** tab. Leave the **SharePoint admin center** tab open as you will use it in the next lab exercise.

21 Proceed to Lab 3 - Exercise 3

22 Module 4 - Lab 3 - Exercise 3 - Create a Ticketing System in SharePoint

As Adatum begins its transition to Microsoft 365 as their hosted cloud solution, they want to use this opportunity to reduce the amount of third-party software products they currently use. This will help them achieve their goal of reducing their overall IT expenses. The CTO has asked Holly Dickson, Adatum's Enterprise Administrator,

to design a solution that uses Microsoft 365 services to replace the third-party IT service request system that Adatum currently uses.

Because Holly is busy with running the Microsoft 365 pilot project along with her other admin responsibilities, the CTO has authorized her to hire an IT consultant to design the new service request ticketing system. However, he doesn't want the consultant to have access to their entire Adatum system, so he wants Holly to implement "good security practices" by only providing the consultant with access to Adatum's IT pilot project environment.

22.1   Important: Collaboration with an External User

In Lab 1, your instructor assigned you the tenant suffix ID of a fellow student in your class. Your fellow student's tenant ID will represent the IT Consultant who will partner with Holly Dickson in building Adatum's new service request ticketing system. In this lab, you will provide your fellow student's tenant ID with access to the new ticketing system. In a lab 1 exercise, you authorized external access to your tenant from this student's tenant ID. By providing external access to this tenant suffix ID, you and your fellow student will be able to collaborate through Microsoft Teams as you set up this new service request ticketing system (you will do this in the next lab that deals with Teams).

In the previous lab exercise, you created a SharePoint team site called IT Services. As you develop this site, you will employ good security practices by limiting site access to Holly and your fellow student's tenant ID (this tenant ID represents the IT consultant). As you set up the new service request ticketing system, you will access the site using your fellow student's tenant ID to prove that the IT consultant can access the system. In the next lab involving Microsoft Teams, you will actually chat with your fellow student concerning the new ticketing system. Keep in mind that the student who was assigned as your IT consultant will also be taking on the role of Holly Dickson in his or her own lab, and you will be taking on the IT consultant role with another student. Therefore, each student in the class will take on dual roles – that of Holly Dickson in the student's own lab, and that of the IT consultant for a fellow student's lab.

22.1.1   Task 1 - Assign site permissions to your IT consultant

As Holly Dickson, you earlier provided your fellow student's tenant ID with External Access back in Lab 1. You now must assign the consultant with permission to access the new IT Services team site that you created in the prior lab. If you will recall, in the prior lab you created a new Information Technology group that was assigned to the IT Services site. This group included Isaiah Langer and Joni Sherman, and you assigned the group Full Control permissions. Since you do not want the IT consultant to have Full Control permissions, you do not want to assign the consultant to the Information Technology group.

Instead, in your role as Holly Dickson, you will perform the following steps in this task to assign the IT consultant to the IT Services team site with limited permissions:

- You will create a new permission level for the IT Services site titled **Restricted Use**. You will then assign to this permission level the limited set of permissions that you want assigned to any external users who will access the site (in this case, the IT Consultant).
- For the IT Services site, you will then create a new group of users titled **Consultants**, and you will assign your fellow student's tenant admin account (which represents the IT Consultant) to this group.
- You will assign the **Restricted Use** permission level to this **Consultants** group. This will limit the actions the IT Consultant will be able to perform when accessing the IT Services site.

1. You should meet with the student who your instructor assigned to your lab to play the role of the IT consultant. During this meeting you should exchange the tenant admin accounts (**admin@xxxxxZZZZZZ. onmicrosoft.com**) from each of your tenants along with the tenant admin's password.

2. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

3. You should still have your Edge browser and the SharePoint admin center open from the prior lab in which you were logged in as Holly Dickson. If so, proceed to the next step; otherwise, navigate to the SharePoint admin center just as you did in the prior lab exercise.

4. In the **SharePoint admin center**, you will begin by creating a new permission level for the IT Services site. In the left-hand navigation pane, select **Sites**, and then select **Active sites**.

5. In the list of **Active sites**, locate the **IT Services** site and then select the **.../sites/ITServices** value that appears in the URL column for this site.

6. A new tab will open in your Edge browser that displays the **IT Services** site. In the upper right-hand corner of the **IT Services** site, select the **gear (Settings)** icon.

7. In the **Settings** pane that appears, select **Site permissions.**

8. At the bottom of the **Site permissions** pane, select **Advanced permissions settings**, which opens a **Permissions: IT Services** page.

9. In the ribbon that appears at the top of the screen, the **PERMISSIONS** tab is displayed by default. Under the **Manage** section, select **Permission Levels.**

10. In the **Permissions > Permission Levels** page, on the menu bar that appears above the list of permission levels, select **Add a Permission Level**.

11. In the **Permission Levels > Add a Permission Level** page, enter the following information:

    - Name: **Restricted Use**

    - Description: **This level restricts the level of use inside the IT Services site.**

    - When selecting the permissions, do NOT select the **Select All** Instead, select the following limited set of permissions under the **List Permissions** section:

        – **Manage lists** (which selects **View Items**)
        – **Add items**
        – **Edit items**
        – **View versions** (which selects **Open Items**)
        – **View Application Pages**

    - Select the following permissions under the **Site Permissions** section:

        – **Add and Customize Pages** (which selects **Browse Directories, View Pages**, and **Open**)
        – **Use Self-Service Site Creation** (which selects **Browse User information**)
        – **Use Remote interfaces**
        – **Use Client integration features**

12. Scroll to the bottom of the page and select the **Create** button to create the new **Restricted Use** permission level.

13. Once the permission level is created you will be redirected to the **Permissions > Permission Levels** page. Verify the new **Restricted Use** permission level appears in the list of permission levels for this IT Services site.

    On this **Permissions > Permission Levels** heading line, select the **Permissions** link to return to the **Permissions: IT Services** page.

14. In the ribbon displayed at the top of the screen, the **PERMISSIONS** tab is displayed by default. In this tab, under the **Grant** section, select **Create Group**.

15. On the **People and Groups > Create Group** page, enter the following information:

    - Name: **Consultants**

    - About Me: **This group is used for allowing consultants to modify work products only**.

    - Who can view the Membership of the Group: **Everyone**

    - Who can edit the membership of the Group: **Group Owner**

    - Allow requests to Join/leave this group: **No**

    - Auto-accept requests: **No**

    - Choose the permission level group members get on this site: **Restricted use – This level restricts the level of use inside the IT Services site**

        Note: This setting includes the **Designer** permission level that you created in the prior lab and the **Restricted Use** permission level that you just created in this task. You will only assign this group the **Restricted Use** permission level.

16. Select **Create**. You will be redirected to the **People and Groups > Consultants** page for this **Consultants** group.

17. On the menu bar that appears above the list of consultants, select the drop-down arrow next to **New**. In the menu that appears, select **Add Users.**

18. In the **Share 'IT Services'** window that appears, in the **Enter names or email addresses** field, enter your fellow student's tenant admin account, which will be **admin@xxxxxZZZZZZ.onmicrosoft.com** (**IMPORTANT:** replace xxxxxZZZZZZ with your fellow student's tenant prefix that was assigned to you by your instructor; do **NOT** use your tenant prefix).

    This same address will be displayed below the field in a menu. Select this address.

    Note: A message should appear below this field that says: **admin@xxxxxZZZZZZ.onmicrosoft.com is outside of your organization.**

19. Select **SHOW OPTIONS.** Note that the **Send an email invitation** option is selected by default. Leave this option selected.

20. Select **Share**.

21. Because you selected the option to **Send an email invitation**, your fellow student will receive an email invitation in his or her MOD Administrator's Inbox. To verify this email was received, you must open an InPrivate browsing session to impersonate your fellow student's tenant. This enables you to access your fellow student's MOD Administrator account within the student's tenant, and therefore access this MOD Administrator's Outlook Inbox.

    On your taskbar, right-click on the **Microsoft Edge** icon and select **New InPrivate window** in the menu that appears.

22. This opens an InPrivate browsing session. Maximize the InPrivate browser window, and then enter the following URL in the address bar: **https://outlook.office365.com/mail/inbox**

23. In the **Sign in** window, enter your fellow student's MOD Administrator email address of **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is your fellow student's tenant prefix that was assigned to you by your instructor). In the **Enter password** window, enter your fellow student's tenant email password and select **Sign in**.

24. In the **Stay signed in?** dialog box, select **Yes**.

25. This will open your fellow student's MOD Administrator's Inbox in Outlook. In the Inbox you should see an email from **no-reply@sharepointonline.com.** Open the email.

26. In the email, it will display **Go To IT Services**. The **IT Services** portion of this message is hyperlinked. Select **IT Services**.

27. A new tab will open in your InPrivate browsing session that displays **Welcome to SharePoint Online.** On this webpage, select **Organizational account.**

28. This will open the **IT Services** site that you created in your tenant. In other words, by using an InPrivate browsing session, you are impersonating your fellow student by being signed into his or her tenant, and from your fellow student's browser (i.e. in the InPrivate browsing session), you are accessing the **IT Services** site that Holly created in Adatum's Microsoft 365 tenant.

29. On the **IT Services** site, in the left-hand navigation pane, select **Documents**.

30. On the **Documents** page, select **+New** on the menu bar. In the drop-down menu that appears, you should see all the objects the IT Consultant can create in this site.

31. Select the X in the upper right corner of the screen to close the InPrivate Browsing session in Microsoft Edge.

32. Close the Microsoft Outlook mail message that you opened earlier.

33. This will return you to the **People and Groups > Consultants** site in your normal Edge browser session. If your fellow student's MOD Administrator account does not appear in the list of consultants, select the **Refresh** icon on the left-side of the address bar at the top of the page to refresh the list. Your fellow student's **MOD Administrator** account should now appear.

34. Leave the browser open and proceed to the next task.

22.1.2 Task 2 - Upload existing ticket request data (IT Consultant steps)

In this task, **you will take on the persona of the IT consultant** who is helping Holly Dickson implement a new service request ticketing system. In your role as the IT consultant, you are concerned that during this transition from Adatum's old ticketing system to the new one, Adatum may lose critical historical data, such as ticket volume and monthly activity. Therefore, you have recommended to Holly that you should upload the existing data from Adatum's old service request ticketing system to the new ticketing system.

To facilitate this process, the existing ticketing data has been captured in a spreadsheet and a backup spreadsheet, and your lab service provider has stored these two spreadsheets on LON-CL1.

As the IT Consultant in this task, you will perform two primary steps:

- You will connect to Adatum's IT Services team site to validate that you can access the site and authenticate your credentials.

- You will export the existing ticket data from the spreadsheet on LON-CL1 and upload it to a SharePoint list in the IT Services site that Adatum (Holly) created in the prior task. When the data is uploaded to the IT Services site, it will be uploaded as a SharePoint list (titled "Service Desk Requests") on the site.

  IMPORTANT: There are two ways in which you can export the data from the spreadsheet and upload it to the SharePoint list on the IT Services site: through commands in the Excel spreadsheet, or by running a PowerShell script. Both options are presented in this task and you are free to choose whichever method you prefer. Using the Excel spreadsheet commands is probably the more common method, but for those of you who prefer to work in PowerShell, using the PowerShell script provides another experience to add to your personal repository of PowerShell tools.

CAUTION: In this task, whenever you access the URL of the IT Services site, you will use **your** tenant prefix (xxxxxZZZZZZ) in the URL (**https://xxxxxZZZZZZ.sharepoint.com/sites/ITServices**), since you created the site in your Adatum tenant in the prior task. When you access this site in your role as the IT Consultant, you will sign in using your fellow student's tenant admin username and password (which represents the IT Consultant); the username will be **admin@xxxxxZZZZZZ.onmicrosoft.com**, where the tenant prefix (xxxxxZZZZZZ) will be **your fellow student's** tenant prefix that was assigned to you by your instructor.

1. Switch to **LON-CL1**.

2. On **LON-CL1**, you should still be logged in as the **Administrator** (Adatum\Administrator) from the earlier lab in which you installed Microsoft 365 Apps for enterprise. If you did not log out of LON-CL1 as Laura Atkins and log back in as the Administrator at the end of the earlier lab, then do so now.

3. Select the **File Explorer** icon that is located on the taskbar at the bottom of the screen.

4. Maximize the **File Explorer** window, and then select the **Documents**.

5. If you will recall from the task description, you will be presented with two options for completing this task: through commands in the Excel spreadsheet, or by running a PowerShell script.

   - If you prefer to use Excel to accomplish this task, then proceed to **step 6**.
   - If you prefer to use PowerShell, then proceed to **step 25**.

6. **START HERE TO PERFORM THIS TASK USING EXCEL.**

   Since you are at this step, you have chosen to use Excel to export the table data into a SharePoint list in the IT Services site.

   Open **File Explorer** and under **This PC**, select **Documents** (this provides a shortcut that points to the actual path of C:\Users\Administrator.ADATUM\Documents). Confirm the **Service Request System.xlsx** and **BackupFile.xlsx** files are present in the Documents folder. The **Service Request System** spreadsheet contains copies of the service request tickets from Adatum's old ticketing system. The **Backup File** spreadsheet, which is simply a copy of the Service Request System file, was created for precautionary purposes (it will come into play in the next task). Note that there are two files with the name **Service Request System**; one is an Excel spreadsheet file with a .xlsx extension, and the other is a comma separated value file with a .csv extension. The Excel spreadsheet file is used in this section, whereas students that chose to use PowerShell will use the .csv file.

   Double-click the **Service Request System.xlsx** file to open it. Make sure you open the .xlsx file and not the .csv file.

7. If a **Sign in to set up Office** window appears, sign in using the tenant admin account (admin@ xxxxxZZZZZZ.onmicrosoft.com, where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and tenant admin password.

8. If an **Accept the license agreement** window appears, select the **Accept** button.

9. If a **Your privacy option** window appears, select the **Close** button at the bottom of the window.

10. In the next several steps, you will verify that in your role as the IT Consultant, you can connect to the IT Services site and that you can authenticate access to the site using your tenant admin's credentials. Even though you will use the Excel command to **Get Data** from another source and import it into your spreadsheet, you will actually NOT being doing that since you already have the data in the spreadsheet. You will simply use this **Get Data** command to verify that you can successfully access the IT Services site from your PC.

    In **Excel,** in the menu bar at the top of the screen, select **Data**.

11. In the ribbon, under the **Get and Transform Data** section, select the **Get Data** drop-down arrow. In the menu that appears, select **From Online Services**, and then in its menu, select **From SharePoint Online list**.

12. A new **SharePoint Online lists** window will open. In the **Site URL** field, enter **https://xxxxxZZZZZZ.sharepoint** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider, since the IT Services site is on your tenant).

    Note: Before you select **OK**, copy the site URL that you just entered as you will need to enter this in future steps. Copying it now will save you from having to manually enter it later.

    Select **OK**.

13. If a dialog box appears that allows you to select the type of authentication you want to use to access the IT Services site, it will display three options in the left-hand pane: Anonymous, Windows, and Microsoft account. Anonymous is displayed by default. However, in this case, select **Microsoft account**.

    The dialog box displays a message indicating **You aren't signed in**. Select the **Sign in** button.

    On the **Pick an account** window, select **Use another account** because you want to sign in as the IT Consultant's tenant admin account (**admin@xxxxxZZZZZZ.onmicrosoft.com** where xxxxxZZZZZZ is **your fellow student's tenant prefix that was assigned to you by your instructor**). In the **Enter password** window, enter your fellow student's tenant password and then select **Sign in**. If your sign in is successful, a message will be displayed in the window indicating you are signed in.

    Once you are signed in, select **Connect**.

14. When the **Navigator** window appears, this is your indication that you have established a connection between the IT Consultant's external user account and Adatum's IT Services site that Holly created in the prior task. Even though you used the **Get Data** command in Excel to do this, you will NOT import any data locally to the Excel spreadsheet (the data is already in the spreadsheet).

    Select **Cancel** to close the **Navigator** window.

15. Now that you have verified that the IT Consultant's external user account can access the IT Services site, you will export Adatum's existing ticketing system data from the spreadsheet and upload it as a SharePoint list into the IT Services site.

    If you are already familiar with the use of table objects in Excel, **select a cell in the table and proceed to the next step.**

    However, if you are not that familiar working with tables in Excel, note how the final two menu bar options are **View** and **Help**. You are now going to select the table in the spreadsheet, and after doing so, you will note the changes to the menu bar.

    Before you can export an Excel table into a SharePoint list, the stationary list of data must be inserted into an Excel table object. This has already been done for you as the data in the spreadsheet has already been inserted into an Excel table object. All you must do now is select the table, which can be done by simply selecting any cell of data (for example, select cell **C3**).

    Because you have now selected the Excel table, note how the new menu bar option titled **Table Design** appears after **Help**.

Note: If you select a cell outside of the table, note how the **Table Design** menu bar option disappears. If you once again select a cell inside the table, note how it reappears.

16. On the menu bar, select **Table Design**.

17. In the ribbon, under the **External Table Data** section, select the **Export** drop-down arrow. In the menu that appears, select **Export Table to SharePoint List**.

18. An **Export Table to SharePoint List – Step 1 of 2** window will appear. Enter the following information:

   - **Address:** If you copied the IT Services site URL from the earlier step, then paste that in now; otherwise, enter **https://xxxxxZZZZZZ.sharepoint.com/sites/ITservices** (where xxxxxZZZZZZZ is **your tenant prefix** provided by your lab hosting provider).

     Important: By default, the Address field is prefilled with "http://". If you manually enter the URL, you must change this to "https://"; otherwise, your connection to the IT Services site will fail.

   - **Name:** This is the name of the new distribution list that will be created in this site. For Adatum's new ticketing system, enter **Service Desk Requests**.

   - **Description:** (optional) – leave blank

19. Select **Next**.

20. An **Export Table to SharePoint List – Step 2 of 2** window will appear. Review the information and then select **Finish**.

21. A **Microsoft SharePoint Foundation** dialog box will appear that indicates the table was successfully published.

   Important: Do NOT select OK; instead, select the **link** to the site in which the table was published. This will take you to the IT Services site where it will display a list showing the data that was exported from the spreadsheet and uploaded into the site.

   Note: If a **Sign in** window appears, enter the MOD Administrator's account for the IT Consultant's tenant. In this case, enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZZ is your fellow student's tenant prefix that was assigned to you by your instructor). Select **Next**, and then in the **Enter password** window, enter your fellow student's tenant password and then select **Sign in**.

22. On the taskbar at the bottom of the screen, select the **Excel** icon. In the **Microsoft SharePoint Foundation** dialog box that displayed the link to the published list in the IT Services site, select **OK** to close the window.

23. Close Excel.

24. Close your Edge browser.

   Important: This completes the steps involved in using Excel to export the table data into a SharePoint list (Service Desk Requests) in the IT Services site. **You should SKIP the remaining steps in this task and proceed to the next task.**

25. **START HERE TO PERFORM THIS TASK USING POWERSHELL.**

   Since you are at this step, you have chosen to use Windows PowerShell to export the table data into a SharePoint list in the IT Services site rather than using Excel to accomplish this task.

   Open **File Explorer** and under **This PC**, select **Documents** (this provides a shortcut that points to the actual path of C:\Users\Administrator.ADATUM\Documents). Confirm the **Service Request System.csv** file is present in the Documents folder. This file contains copies of the service request tickets from Adatum's old ticketing system. Note that there are two files with the name **Service Request System**; one is this comma separated value file with a .csv extension, and the other is an Excel spreadsheet file with a .xlsx extension. The .csv file is used in this section, whereas students that chose to use Excel to complete this task will use the .xlsx file. The **Backupfile.xlsx** spreadsheet, which is simply a copy of the Service Request System.xlsx file, was created for precautionary purposes (it will come into play in the next task).

   Confirm the **ImportCsvToSharepointList.ps1** script is also present in the **Documents** folder. This script contains the PowerShell commands you will run to export the table data from the **Service Request System.csv** file and import it into a SharePoint list in the IT Services site.

26. In the **Search** field on the taskbar at the bottom of the desktop, enter **PowerShell**.

Important: Because you MUST run several of the commands within this script individually rather than running the entire script at once, you should select **Windows PowerShell ISE** (not Windows PowerShell); therefore, right-click on **Windows PowerShell ISE** and select **Run as administrator**.

27. If a **User Account Control** dialog box appears, select **Yes** to allow this app to make changes to your device.

28. In **Windows PowerShell ISE**, in the menu bar, select **File** and then select **Open**. In the **File Explorer** window, navigate to **This PC** and then to the **Documents** folder. Select the **ImportCsvFileToSharepointList.ps1** script and then select **Open**.

29. In the script, you will run the commands in lines **11-13** together; therefore, select these three lines in the script and then select the **Run Selection (F8)** icon on the menu bar. These lines will set your execution policy as Remote Signed and install both the SharePoint Online module as well as the SharePoint PNP module. The PNP module enables you to remotely sign into your SharePoint Online environment and manage your SharePoint lists.

30. If you are prompted to confirm an **Execution Policy Change**, select **Yes to All.**

31. If you are prompted to confirm a **NuGet provider is required to continue**, select **Yes**.

32. If you are prompted to confirm an **Untrusted repository**, select **Yes to All.**

33. If you are prompted a second time to confirm an **Untrusted repository** dialog box, select **Yes to All.**

34. At the command prompt, you will run the commands in lines **20-21** together; therefore, select these two lines in the script and then select the **Run Selection (F8)** icon on the menu bar.

35. In the **Windows PowerShell credential request** dialog box that appears, enter **admin@ xxxxxZZZZZZ.onmicrosoft.com** in the **User name** field (where xxxxxZZZZZZ is the tenant prefix *from your fellow student* that was assigned to you by your instructor); this is the IT Consultant's MOD Administrator (tenant admin) account.

Note: Copy the value (Ctrl+C) that you entered in the **User name** field as you will have to enter it again in a couple of steps. By copying the value here, you can simply paste it in later on rather than re-entering it.

Enter your fellow student's tenant admin password in the **Password** field, and then select **OK**.

36. On line **32** in the script, you MUST update the URL before you can run this command. In the URL, you must replace the xxxxxZZZZZZ with *your tenant ID* provided by your lab hosting provider (this is your Adatum tenant where the IT Services site was created earlier by Holly).

37. At the command prompt, you will run the command in line **32** by itself; therefore, select this line in the script and then select the **Run Selection (F8)** icon on the menu bar.

38. In the **Enter your credentials** dialog box, paste into the **User name** field the value that you copied in the earlier step. If you did not copy the User name value, then enter in the **User name** field **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix *from your fellow student* that was assigned to you by your instructor); this is the IT Consultant's MOD Administrator (tenant admin) account.

Enter your fellow student's tenant admin password in the **Password** field, and then select **OK**.

39. The commands in lines 41-51 in the script MUST be run individually. If you select all six commands and run them all together at one time, the commands will fail.

Therefore, at the command prompt, select line **41** in the script and then select the **Run Selection (F8)** icon on the menu bar. **Note:** This command in row 41 creates a new column in the distribution list that does not exist in the Excel spreadsheet. For each record imported from the spreadsheet into this distribution list, the value of this column will be blank. The reason you must run this command is that this specific column is required to successfully import the data and create the distribution list using PowerShell. That being said, when you create new filtered views later on in Task 4, you will ignore this column and not include it in any of the views you create.

Then select line **43** in the script and select the **Run Selection (F8)** icon on the menu bar.

Repeat this process for the commands in lines **45, 47, 49,** and **51**.

40. At the command prompt, you will run the command in line **60** by itself; therefore, select this line in the script and then select the **Run Selection (F8)** icon on the menu bar.

    Note: This command displays the list of sites in the IT Services site. Verify the Service Desk Requests list appears in this list.

41. At the command prompt, you will run the command in line **66** by itself; therefore, select this line in the script and then select the **Run Selection (F8)** icon on the menu bar. This command displays all the records in the .csv file that were imported into the terminal.

42. In the script, lines **73-79** represent one command; therefore, all these lines must be selected together and run as one selection.

    At the command prompt, select lines **73-79** in the script and then select the **Run Selection (F8)** icon on the menu bar. This command will display a summary each of the rows that were imported from the .csv file.

43. At the command prompt, you have finished running the commands in this script. Close Windows Power-Shell.

44. Open your Edge browser and enter the following URL in the address bar to navigate to the **IT Services** site: **https://xxxxxZZZZZZ.sharepoint.com/sites/ITServices** (where xxxxxZZZZZZ is *your tenant prefix* provided by your lab hosting provider).

45. In the **IT Services** site, in the left-hand pane, select **Site contents**. In the list of Site contents, select the **Service Desk Requests** item.

46. This displays the **Service Desk Requests** list. Review the 30 items in the list, which should match the 30 items in the .csv file.

47. Close Windows PowerShell.

48. Close your Edge browser and proceed to the next task.

22.1.3 Task 3 - Add Additional Columns to the SharePoint list

In this task you will return to your role as Holly Dickson. You have just been informed by the IT Consultant that he or she finished exporting the existing ticketing system data and uploaded it to the new SharePoint site. However, as you reviewed the list of data that was imported into the Service Desk Requests list, you noticed that the **Customer** field and the **Assign to** fields were missing. The **Customer** field is the name of the person who entered the ticket, and the **Assign to** field is the name of the support engineer to whom the ticket was assigned. This is critical data for a service request system, so it is imperative that you add this information to the **Service Desk Requests** list.

1. On LON-CL1 you should have closed the Edge browser at the end of the prior task. If not, then do so now.

2. Since Holly will be using her PC to perform this task, you will use LON-CL1 in this role-playing exercise as Holly's PC rather than the IT Consultant's PC as you did in the prior task.

   Select the **Microsoft Edge** icon on the taskbar to open your browser, and then enter the following URL in the address bar: **https://portal.office.com**.

3. In the **Pick an account** window, select Holly's account if it appears; otherwise, select **Use another account** and then enter **holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix assigned to you by your lab hosting provider). In the **Enter password** window, enter **Pa55w.rd** and select **Sign in**.

4. After reviewing the data that was imported into the Service Desk Requests list, you noticed that the **Customer** field and the **Assign to** fields were missing. However, after reviewing the spreadsheet, you realized the missing data wasn't an upload issue because the **Customer** and **Assign To** columns were missing from the spreadsheet.

   While you cannot explain what caused this, you remember making a backup of the original spreadsheet. If these missing columns are in your backup file, you plan to add the two columns from your backup file to the **Service Desk Requests** list that is displayed in the IT Services site.

   Select the **File Explorer** icon on the taskbar to return to the **Documents** folder that you opened in the prior task. Double-click on the **Backupfile.xlsx** file to open it.

5. Review the columns in the table and verify the **Assign to** and **Customer** columns appear. Since you have just verified that this data was captured in your backup file, you can proceed with adding these columns to the **Service Desk Requests** list.

6. In your Edge browser, in the **Office 365 home** page, select the **SharePoint** icon in the column of Microsoft 365 app icons on the left-side of the screen.

   If a **Pick an account** window appears, select Holly's account.

7. A **News from sites** window appears over top of the SharePoint admin center. Close this window.

8. On the **SharePoint admin center**, in the left-hand navigation pane, scroll down and under the **Recent** group, select **IT Services**.

9. On the **IT Services** site, near the bottom of the left-hand navigation pane, select the **X** above **Microsoft Teams** to hide this banner, and in the **Hide** dialog box, select **Yes** to confirm it.

   In the left-hand navigation pane, select **Site Contents**, and in the **Contents** list, select **Service Desk Requests**. You want to create a new column to display the **Customer** data that you will import from the **Backupfile.xlsx** spreadsheet.

10. On the menu bar at the top of the page, the option to the right of the **+New** button will either display **Edit in grid view** or **Exit grid view**. This option allows you to toggle in or out of grid view. You do NOT want to be in grid view to edit the list.

    If this option displays **Edit in grid view**, it means you are not in grid view, so proceed to the next step.

    If this option displays **Exit grid view**, then you are currently in grid view, which you do not want to be in. In this case, select **Exit grid view**.

11. At the end of the column heading row, select **+Add column**, and then in the drop-down menu that appears, select **Person**.

12. In the **Create a column** window that appears, enter **Customer** in the **Name** field.

13. In the **Type** field, verify it's already set to **Person or Group**.

14. Verify the **Allow selection of Groups** check box is NOT selected. Do NOT select this check box.

15. Select **More options**.

16. Select the **Require that this column contains information** toggle switch to change it to **Yes**.

17. Select **Save**.

18. The **Customer** column should appear in the list. All record entries for this column should be highlighted in yellow and **Required info** should appear in this column for each record (this is because you set the **Require that this column contains information** option to **Yes** in the previous step when you created this column).

19. Earlier, you were instructed to not be in grid view to add the Customer column. However, now that you have added the column, you must switch to grid view to copy and paste in the Column data from the Backupfile.xlsx spreadsheet.

    On the menu bar, select **Edit in grid view**. In the next few steps, you will copy the Customer data from the **BackupCopy** spreadsheet and paste it into this column in the SharePoint list.

20. Select the **Excel** spreadsheet icon on the taskbar to display the **BackupFile.xlsx** spreadsheet. Select all the items in the **Customer** column (start in row 2 so that you do not copy the column header), then right-click and select **Copy** from the menu (NOTE: Use the Copy option here instead of **Ctrl+C** to copy the column data; Ctrl+C sometimes results in an error when you attempt to paste in the copied cells in the next step).

    Note: If a window appears showing the progress of the Copy command, do NOT proceed until the pane disappears. This may take a minute or so for the copy process to complete. If a progress window does not appear, then proceed to the next step.

21. Select the **Edge** browser icon on the taskbar, which should return you to the grid view page for the **Service Desk Requests** list. Select all the empty fields in the **Customer** column and press **Ctrl+V**. All items will automatically appear in the appropriate row for the **Customer** column.

22. Select the **Exit grid view** option on the menu bar to see how the Customer data appears in normal display view.

23. Repeat steps **11-22** to add a column for the **Assign To** data and to copy the **Assign to** data from the **BackupFile.xlsx** spreadsheet and paste it into the **Service Desk Requests** list.

24. After reviewing the changes to the **Service Desk Requests** list, you realize that the data type of the **Description** column only supports a **single line of text**. While this is fine for the existing data, going forward you want your customer support engineers to be able to enter more detailed information. Therefore, you want to modify this column to change the data type to **multiple lines of text**.

    To make this change, select the **Description** column heading. In the menu that appears, select **Column Settings**, and then in the sub-menu, select **Edit**.

25. In the **Edit column** window, select the drop-down arrow in the **Type** field and select **Multiple lines of text**.

26. Select **More options**.

27. Change the **Require that this column contains information** option to **Yes**.

28. Select **Save**.

29. Leave the browser and all existing tabs open on LON-CL1 for the next task.

22.1.4 Task 4 - Create filtered views for targeted viewing

In this task, you will continue in your role as Holly Dickson, Adatum's Enterprise Administrator. You were just informed by your IT Consultant that while the default **All items** view in the **Service Desk Requests** list will display all the existing service tickets, this will not help the Customer Support Manager when she wants to focus on specific groups of cases. To address this issue, the IT Consultant has recommended that you create the following new filtered views to provide this visibility:

- Active cases by Support Agent
- Closed cases by Support Agent
- All Cases by Support Agent
- All Cases by Customer

1. You should still be signed into LON-CL1 as the **Administrator**, and you should be logged into Microsoft 365 as Holly Dickson. In your browser, you should still have the tab open from the prior task that displays the **Service Desk Requests** list. If not, then navigate to this list now.
2. You will begin by creating a view showing all active cases. On the **Service Desk Requests** page, select the **gear** (**Settings**) icon in the top right corner of the webpage. In the menu that appears, select **List settings.**
3. In the **Service Desk Requests > Settings** page, scroll down to the bottom of the page and in the **Views** section, select **Create view.**
4. In the **Settings > View Type** page, select **Standard view.**
5. In the **Settings > Create View** page, enter the following information:
   - View Name: **Active Cases by Support Agent**
   - View Audience: **Create a Public View**
   - In the list of Columns, you must first uncheck all the columns currently selected. Then you MUST select the following columns **in the order they appear below**, which is in ascending **Position from left** sequence. If you select them as you progress from top to bottom in the list on the page, the system will automatically adjust the **Position from left** values to different values:
     - **Assign To** – Position from left: **1**
     - **Date** – Position from left: **2**
     - **Customer** – Position from left: **3**
     - **Location** – Position from left: **4**
     - **issueTitle** - Position from left: **5**
     - **Description** – Position from left: **6**
   - Sort section - First sort by the column: **Assign to** and **Show items in ascending order**
   - Then sort by the column: **Date** and **Show items in ascending order**
   - Filter section - **Show items only when the following is true**
   - Show the items when column section – select **Issue status** column
   - Operand field – **Is equal to**
   - Condition field – enter **Active**

6. Scroll to the bottom of the page and select **OK**.
7. You will now create a view showing all closed cases. On the **Service Desk Requests** page, select the **gear** (**Settings**) icon in the top right corner of the webpage. In the menu that appears, select **List settings.**
8. In the **Service Desk Requests > Settings** page, scroll down to the **Views** section and select **Create view.**
9. In the **Settings > View Type** page, select **Standard view.**
10. In the **Settings > Create View** page, enter the following information:
    - View Name: **Closed Cases by Support Agent**
    - View Audience: **Create a Public View**
    - In the list of Columns, you must first uncheck all the columns currently selected. Then you MUST select the following columns **in the order they appear below**, which is in ascending **Position from left** sequence. If you select them as you progress from top to bottom in the list on the page, the system will automatically adjust the **Position from left** values to different values:
        – **Assign To** – Position from left: **1**
        – **Customer** – Position from left: **2**
        – **Location** – Position from left: **3**
        – **issueTitle** - Position from left: **4**
        – **Description** – Position from left: **5**
    - Sort section - First sort by the column: **Assign to** and **Show items in ascending order**
    - Filter section - **Show items only when the following is true**
    - Show the items when column section – select **Issue status** column
    - Operand field – **Is equal to**
    - Condition field – enter **Resolved**
11. Scroll to the bottom of the page and select **OK**.
12. You will now create a view showing all cases for each support agent. On the **Service Desk Requests** page, select the **gear** (**Settings**) icon in the top right corner of the webpage. In the menu that appears, select **List settings.**
13. In the **Service Desk Requests > Settings** page, scroll down to the **Views** section and select **Create view.**
14. In the **Settings > View Type** page, select **Standard view.**
15. In the **Settings > Create View** page, enter the following information:
    - View Name: **All Cases by Support Agent**
    - View Audience: **Create a Public View**
    - In the list of Columns, you must first uncheck all the columns currently selected. Then you MUST select the following columns **in the order they appear below**, which is in ascending **Position from left** sequence. If you select them as you progress from top to bottom in the list on the page, the system will automatically adjust the **Position from left** values to different values:
        – **Assign To** – Position from left: **1**
        – **Customer** – Position from left: **2**
        – **issueTitle** - Position from left: **3**
        – **Location** – Position from left: **4**
        – **Issue Status** – Position from left: **5**
        – **Description** – Position from left: **6**
    - Sort section - First sort by the column: **Assign to** and **Show items in ascending order**
    - Then sort by the column: **Customer** and **Show items in ascending order**
    - Filter section - **Show all items in this view**
16. Scroll to the bottom of the page and select **OK**.
17. You will finish this task by creating a view showing all cases for each customer. On the **Service Desk Requests** page, select the **gear** (**Settings**) icon in the top right corner of the webpage. In the menu that appears, select **List settings.**
18. In the **Service Desk Requests > Settings** page, scroll down to the **Views** section and select **Create view.**
19. In the **Settings > View Type** page, select **Standard view.**
20. In the **Settings > Create View** page, enter the following information:
    - View Name: **All Cases by Customer**
    - View Audience: **Create a Public View**
    - In the list of Columns, you must first uncheck all the columns currently selected. Then you MUST select the following columns **in the order they appear below**, which is in ascending **Position from left** sequence. If you select them as you progress from top to bottom in the list on the page, the system will automatically adjust the **Position from left** values to different values:

- **Customer** – Position from left: **1**
- **Date** – Position from left: **2**
- **Assign To** – Position from left: **3**
- **issueTitle** - Position from left: **4**
- **Location** – Position from left: **5**
- **Issue Status** – Position from left: **6**
- **Description** – Position from left: **7**
  - Sort section - First sort by the column: **Customer** and **Show items in ascending order**
  - Then sort by the column: **Date** and **Show items in ascending order**
  - Filter section - **Show all items in this view**
21. Scroll to the bottom of the page and select **OK**.
22. In your Edge browser, close all tabs EXCEPT for the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab.

Congratulations! You have completed the building blocks for your new Service Desk Ticketing system. You will add additional functionality to the ticketing system in later labs.

22.2   Proceed to Lab 3 - Exercise 4

23   Module 4 - Lab 3 - Exercise 4 - Review Key Features of Microsoft Teams

In this exercise you will learn how to manage and configure teams through the Microsoft Teams admin center.

23.0.1   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**; if not, then do so now.

2. On LON-DC1, you should still have your Edge browser and the **Microsoft 365 admin center** open from the prior lab. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and **Pa55w.rd**, and then in the **Microsoft Office Home** page, select the **Admin** icon to open the Microsoft 365 admin center.

3. To start fresh in this Teams lab exercise, close all SharePoint-related tabs in your Edge browser that were left open from the previous SharePoint lab exercise. Only leave the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab open.

4. In the **Microsoft 365 admin center** tab, in the left-hand navigation pane under the **Admin centers** section, select **Teams.** This will open the Microsoft Teams admin center.

5. In the **Microsoft Teams admin center**, in the left-hand navigation pane, select **Meetings** and then in the drop=down menu, select **Meeting policies**.

6. In the **Meeting policies** window, scroll down to the list of meeting policies and select **Global (Org-wide default)**.

7. In the **Global** window that appears, under the **General** section, review each setting. All settings in this section should be turned **On**.

8. Under the **Audio & video** section, review each setting. Select the **Allow transcription** toggle switch to turn it **On**.

9. Under the **Content Sharing** section, review each setting and make the following changes:

Set the **Screen sharing mode** to **Single application**. Set the **Allow an external participant to give or request control** setting to **On**.

10. 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 verify the **Allow dial-in users to bypass the lobby** option is set to **Off**; if this option is turned On, then change it 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.

11. Scroll to the bottom of the page and select **Save**.

12. Leave all tabs open in your browser and proceed to the next task.

23.0.2 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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, under the **Meetings** group in the left-hand navigation pane, select **Meeting settings.**

3. On the **Meetings settings** page, under the **Email invitation** section, enter the following information:

   - Logo URL: **https://adatum.com/media/adatumlogo.png** (Hint: copy **https://adatum.com/** so that you can paste it into the next two URLs; this will save you from having to type that portion of the URL each time)

   - Legal URL: **https://adatum.com/legal.html**

   - Help URL: **https://adatum.com/joiningmeetinghelp.html**

   - Footer: **Please accept at your earliest convenience. Thank you!**

4. Select the **Preview invite** button.

5. Review the preview image of the invitation and then scroll down to the bottom of the preview window and select **Close**.

6. 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.

7. Scroll to the bottom of the page and select **Save**.

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

23.0.3 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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, select **Messaging policies** in the left-hand navigation pane.

3. In the **Messaging policies** window, only the **Global (Org-wide default)** policy exists. Select **+Add** in the menu bar that appears above the list of policies.

4. Select the **New messaging policy** field at the top of the page and enter **Chat and Channel Messaging Policy** as the name of the policy.

5. 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: **Off**

6. Select **Save.**

7. Leave all tabs open in your browser and proceed to the next task.

23.0.4   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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, select **Org-wide Settings** in the left-hand navigation pane and then select **Resource accounts.**

3. In the **Resource accounts** window, select **+Add** in the menu bar at the top of the page.

4. 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 **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)

   - Resource account type: **Call queue**

5. Select **Save**. **Calling Queue 1** will now appear in the list of **Resource accounts**.

6. Leave all tabs open in your browser and proceed to the next task.

23.0.5   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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, select **Voice** in the left-hand navigation pane and then select **Call queues.**

3. In the **Call queues** window, select **+Add** in the menu bar at the top of the page.

4. Select the **Call queue name** field at the top of the page and enter **Call Queue 1** as the name of the queue.

5. The page displays a message indicating **You haven't added any resource accounts yet.** Below this message, select the **Add accounts** button.

6. In the **Add account** pane that appears on the right-side of the screen, in the **Search by display or username** field, enter **Calling.** As you type **Calling**, a window appears that displays 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.

7. 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.

8. In the **Call Queue 1** window, scroll down the page and select the following values for each option:

   - Language: **English (United States)**

   - 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 **Search by display name or username** field, 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. Select anywhere in the red error message to close the **Add users** pane, and then select the **X** on the right-side of this 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 **Search by distribution list or group name** field, enter **Inside.** As you type Inside, a window appears listing the groups whose name starts with Inside. As you hover your mouse over **Inside Sales**, an **Add** button appears to the right of it. Select the **Add** button.

     In the **Add call agents** pane, the Inside Sales group 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** (Hint: 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**

9. 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.

10. Leave all tabs open in your browser and proceed to the next task.

23.0.6 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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, select **Voice** in the left-hand navigation pane and then select **Calling policies.**

3. 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.

4. Select the **Add new calling policy** field at the top of the page and enter **Default Adatum Calling Policy** as the name of the policy.

5. 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**

6. 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 in the list.

7. Leave all tabs open in your browser and proceed to the next task.

23.0.7   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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, select **Org-wide settings** in the left-hand navigation pane and then select **External access.**

3. In the **External access** window, leave the two settings involving Skype for Business/Teams and Skype users set to **On**. Also note that in the list of domains, the domain of the IT Consultant who helped formulate the new Service Request Ticketing system (**xxxxxZZZZZZonmicrosoft.com**) appears in the list, and that communication is Allowed with this domain. You added this domain back in Lab 1.

4. To add the domain in which you want to allow communication, select **+Add a domain** in the menu bar that appears above the list.

5. In the **Add a domain** window, enter the following information:

   - Domain: **microsoft.com**
   - Action to take on this domain: **Allowed**

6. Select **Done.**

7. To add the blocked domain, in the **External access** window, select **Add a domain.**

8. 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**

9. Select **Done.**

10. 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.

11. Select **Save.**

12. Leave all tabs open in your browser and proceed to the next task.

23.0.8   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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, under **Org-wide settings** in the left-hand navigation pane select **Guest access.**

3. In the **Guest access** window, set the **Allow guest access in Teams** setting to **On**.

4. 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**

5. 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.

6. Leave all tabs open in your browser and proceed to the next task.

23.0.9 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 be logged in as the Adatum Administrator, and you should still be logged into Microsoft 365 in your Edge browser as Holly Dickson.

2. In your Edge browser, in the **Microsoft Teams admin center**, under **Org-wide settings** in the left-hand navigation pane select **Teams settings.**

3. 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: **Disabled**
   - Email integration
     - – Allow users to send emails to a channel email address: **On**
     - – Accept channel email from these SMTP Domains: **microsoft.com**
   - Files
     - – Citrix files: **On**
     - – DropBox: **On**
     - – 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**

4. Select **Save**. Note the message that displays indicating it can take a few hours for the changes to take effect. This message will eventually disappear.

5. Leave all tabs open in your browser and proceed to the next task.

23.0.10   Task 10 – Configure Chat functionality for the Ticketing System

In this task, you will open the Microsoft Teams desktop application on LON-CL1 and log in as Adatum's MOD Administrator. You will then conduct a brief chat session with the IT Consultant (your fellow student whose tenant ID was assigned to you by your instructor). This will validate that you can use Teams to chat with the IT Consultant whenever necessary to discuss matters concerning the new Service Request Ticketing system.

IMPORTANT: Remember that your instructor assigned your tenant prefix to another student, who is also building a similar ticketing system in his or her lab environment. For that student, you will take on the role of the IT Consultant; therefore, expect to receive a text message from that student, who will do so to validate that Chat functionality is working within his or her Teams' application.

1. Switch to **LON-CL1**. You should still be logged into your LON-CL1 VM as the Administrator with a password of **Pa55w.rd**; if not, then do so now.

2. If the **Microsoft Teams** icon appears on the taskbar, then select it now; otherwise, navigate to the desktop and double-click the **Microsoft Teams** icon. Maximize the Microsoft Teams window (if necessary).

3. You want to sign into Microsoft Teams as Adatum's MOD Administrator. If you receive a log-in screen, then log in as **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), and enter your tenant email password as the **Password**.

   However, if the Teams app opens without displaying the log-in screen, or if Teams was already open, you should check the user icon circle in the upper right corner of the screen. If the circle displays **MA** (for your MOD Administrator), then proceed to the next step.

   If any value other than **MA** is displayed in the circle, then you are not logged in as the MOD Administrator. In this case, select the circle, and in the menu that appears, select **Sign out**. Then proceed through the sign-in process and log in as **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), and enter your tenant email password as the **Password**.

4. In **Microsoft Teams**, in the left-hand navigation pane, select **Chat**.

5. On the very top row on the screen, to the right of the **Chat** command is a **Filter** icon and a **New Chat** icon (a pencil inside a square). Select this **New Chat** icon.

6. This opens a new chat window in the main body of the page. You want to chat with your fellow student; therefore, in the **To: Start typing a name or group** field, enter the IT Consultant's MOD Administrator account of **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is **your fellow student's tenant prefix** that was assigned to you by your instructor) and then press **Enter**.

7. Teams will perform an external search on this user account. It should display the result of this search below the **To:** field. Select this value.

8. This will open a new chat session with the IT Consultant (your fellow student). Send a message to this person and conduct a brief chat session to verify that you can communicate with him or her using the Chat functionality within Teams.

9. When you have finished chatting, leave Teams open and proceed to the next task.

24 Proceed to Lab 3 - Exercise 5

25 Module 4 - Lab 3 - Exercise 5 - Review the Power Platform Admin Center

As Adatum begins its transition to Microsoft 365 as its hosted cloud solution, they want to use this opportunity to examine Microsoft's Power Platform functionality. In your role as Holly Dickson, Adatum's Enterprise Administrator, you have been asked to expand your Microsoft 365 pilot project to include Microsoft's Power Platform. Therefore, your first task towards that goal is to familiarize yourself with the Power Platform admin center, which provides a unified portal for administrators to manage environments and settings for Power Apps, Power Automate, and Power BI.

25.0.1 Task 1 – Review the Power Platform Admin Center

In your role as Holly Dickson, you want to review the Power Platform admin center, which is the go-to destination for administrators who create, manage, and support their Power Platform environments.

1. Switch to **LON-DC1**, where you should still be logged in as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. On **LON-DC1**, you should still have your Microsoft Edge browser and the **Microsoft 365 admin center** open from the prior lab in which you were logged in as Holly Dickson. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and **Pa55w.rd**, and then in the **Microsoft 365 Home** page, select the **Admin** icon to open the Microsoft 365 admin center.

3. In your Edge browser, close all tabs except for the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab. Open a new tab in your Edge browser and enter the following URL in the address bar: **https://make.powerapps.com/home**

4. This opens the **PowerApps** studio. Select the **gear (Settings)** icon on the top right corner of the screen. In the **Settings** pane that appears, select **Admin center**. This opens a new tab that displays the **Power Platform admin center.**

5. In the **Power Platform admin center**, the **Environments** tab in the left-hand navigation pane is displayed by default. In the list of **Environments**, note how there is only one environment, the **Adatum Corporation (default)** environment. Select the **Adatum Corporation (default)** environment and review the information available for this environment.

6. In the navigation pane at the top of the screen (**Environments > Adatum Corporation (default)**), select **Environments**.

7. You have decided to create a new environment. On the menu bar at the top of the screen, select **+New** to create a new environment.

8. In the **New environment** pane that appears, enter the following information:

   - Name: **Adatum-Test**

   - Type: **Sandbox**

   - Region: **United States - Default**

   - Create a database for this environment: **No**

9. Select **Save.**

   Note: Trying to save this new environment record will result in an error message at the top of the window. This message indicates you need at least 1 Gb of database capacity, which is not available in your VM lab environment. Close the **New environment** window.

10. Explore other areas of the **Power Platform admin center**, as desired.

11. When you are finished, close the **Power Platform admin center** tab in your browser.

12. In your browser, leave the **Power Apps** tab open for the next lab exercise.

26 Proceed to Lab 3 - Exercise 6

27 Module 4 - Lab 3 - Exercise 6 - Create a Power App from a SharePoint data source

In an earlier exercise in this lab, Holly created a Service Request Ticketing system to manage service desk requests. The ticketing system consisted of a SharePoint team site titled **IT Services** and a SharePoint list within this site titled **Service Desk Requests**. Holly populated this list with the service request tickets from Adatum's old ticketing system.

Rather than having Adatum's Support team use SharePoint to enter and manage new service tickets, Holly envisions using a Power App to perform this function. Therefore, in this exercise, you will create a Power App that utilizes the **Service Desk Requests** SharePoint list as the data source for the app. Holly will then publish and share the app with the IT Consultant for testing purposes as part of Adatum's pilot project.

27.0.1 Task 1: Review the Service Desk Requests list

Start by familiarizing yourself with the SharePoint list which will serve as the data source for your Power App.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. You should still have Microsoft Edge and the **Microsoft 365 admin center** open from the prior lab in which you were logged in as Holly Dickson. If so, proceed to the next step; otherwise, open Microsoft Edge, navigate to **https://portal.office.com/**, log in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and **Pa55w.rd**, and then in the **Microsoft 365 Home** page, select the **Admin** icon to open the Microsoft 365 admin center.

3. In the **Microsoft 365 admin center**, select **Show all** (if necessary), then scroll down to **Admin centers** and select **SharePoint**. This will open the **SharePoint admin center.**

4. In the **SharePoint admin center**, in the left-hand navigation pane, select **Sites**, and then select **Active sites**.

5. In the list of **Active sites**, locate the **IT Services** site and select the **.../sites/ITServices** value that appears in the URL column.

6. In the **IT Services** site, in the left-hand navigation pane, select **Site contents**.

7. In the list of site contents, select **Service Desk Requests**.

8. Review the columns in this list that you added in the earlier lab exercise. These columns will be used by the Power App that you create.

9. Keep this browser tab open and proceed to the next task.

27.1 Task 2: Create a Power App from a Data Source

Adatum's IT Consultant has informed Holly that by building a Power App from a data source, she will see how easy it is to create a fully functioning app because Power Apps will do all the work for her. In this task, Holly wants to test this out by creating a Power App for entering and managing service tickets using the existing Service Desk Requests SharePoint list as the app's data source.

You can create a Power App through either the Power App portal or through SharePoint. In this task, you will use the Power App portal so that you can become familiar with it. Once you create the Power App, you will add a new record to the Service Desk Requests list using the app, you will edit an existing record using the app, and you will delete a record through the app. In each case, you will verify the corresponding activity occurred in the Service Desk Requests list in the IT Services site in SharePoint. Once you have added, edited, and deleted a record using the Power App, you will save the Power App for Adatum's users to access.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. In Microsoft Edge, the **Power Apps** tab should still be open from the prior exercise; if not, open a new tab in your browser and enter the following URL in the address bar: **https://make.powerapps.com**

3. In the **Power Apps** studio, in the left-hand navigation pane, select **+Create**.

4. On the **Three ways to make an app** page, scroll down to the **Start from data** section and select **SharePoint**.

5. A new browser tap opens that displays the available Connections. A **Hi Holly** dialog box will appear over top of this page. Since your country/region is the United States, select **Get started**.

6. In the **Power Apps** studio, on the **Connections** page, the details pane displays the **SharePoint** connection page. Under the **How do you want to connect to your data?** option, select **Connect directly (cloud services)** and then select the **Create** button.

7. On the left side of the screen, under **Connections**, you will see an available connection for SharePoint. In the detail pane, in the list of **Recent sites**, the **IT Services**– **https://xxxxxZZZZZZ.sharepoint.com/sites/ITser** site should be displayed (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provided).

   Select the **IT Services** – **https://xxxxxZZZZZZ.sharepoint.com/sites/ITservices** site.

8. In the **Choose a list** window that appears, you should select the list that you want to use as the data source for your Power App. In this case, select **Service Desk Requests** and select the **Connect** button at the bottom of the screen.

9. Power Apps will connect directly to that SharePoint list and build a fully functional application using the **Service Desk Requests** list as its data source. When it is finished, a **Welcome to Power Apps Studio** dialog box will appear. Select **See a preview of this app** to preview the app from your browser.

10. A preview of the app will appear as **BrowseScreen1** (see the BrowseScreen1 pane on the right-side of the screen). If the size of the screen is so small that you cannot read it, move the slider at the bottom of the screen to increase the image to a legible size.

11. Now that you have seen how the app will appear, you want to test the app by running it. To run the app, press **F5.**

    Note: If your SharePoint list is already populated with entries, you will see them listed here. In this task, you should see a summary of the 30 records in the Service Desk Requests lists. If you were working with a list that was empty, you would see nothing listed under **Search items**.

12. You now want to test how to add a record to the list. To create a new item, select the **plus (+)** sign that appears at the top right corner of the **Service Desk Requests** app. This opens a data entry form that contains fields mapping to each of the columns in the Service Desk Requests list.

13. In the Service Desk Requests data entry form that apears, enter the following information:

    - Title – **Power App test** (this field only appears if you used PowerShell to create the Service Desk Requests list; it does not appear if you created the list using Excel).

    - Issue Status – **Active**

    - Date - **June**

    - Description – **Test record for the new ticketing system Power App**

    - Location – **Main Office**

    - Issue Title – **Power App test**

    - Customer – leave blank

    - Assign To – enter **Allan**, then select **Allan Deyoung** from the user list that appears

14. To save the record that you just added, select the **check mark** icon that appears at the top right corner of the **Service Desk Requests** app.

    However, instead of the record being saved, note the following error message that is displayed below the **Customer** field, which is also highlighted in a red outline: **An entry is required or has an invalid value. Please correct and try again.**

    Note how the **Customer** field has an asterisk to the left of the field name. This indicates it is a required field, which is why you received the error when you left the field blank.

15. In the **Customer** field, enter **Megan**, then select **Megan Bowen** from the user list that appears.

16. Select the **check mark** icon to save your changes. If the record is accepted, the list of records will be displayed. Scroll down the list and locate your record to verify that it appears.

17. You should now verify that the record has been added in the Service Desk Requests list in the IT Services site. In your Edge browser, select the **IT Services – Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll to the bottom of the list and verify the record appears.

18. Switch back to the **App – Power Apps** tab in your brows. The app should still be running in preview mode; if not, press **F5** on your keyboard to run the app.

19. Now that you have added a record into the Service Desk Ticketing system using the Power App, you want to test how the app works in editing an existing record.

    Select the **right arrow (>)** for any item. This displays the **Details** screen for that item. On this screen, you can either edit the record by selecting the **pencil icon** at the top of the form, or you can delete the record by selecting the **trash can icon**.

    For this record, select the **pencil icon** to edit it. Change any of the fields (**Hint:** to easily identify your change in the Service Desk Requests list, change the **Issue Title** value to **Edit Test** or some other easily identifiable text. When you are done, select the **check mark** icon to save your change.

20. On the **Details** screen that appears, verify the change you made is reflected on the screen.

21. You should now verify that the record has been updated in the Service Desk Requests list in the IT Services site. Select the **IT Services – Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll down through the list and verify the record has been updated.

22. Switch back to the **App – Power Apps** tab in your browser. The app should still be running in preview mode; if not, press **F5** on your keyboard to run the app.

23. You should still be on the **Details** screen for the record that you just updated. Select the **left arrow (<)** that appears at the top of the form. This will return you to the browse screen for the app.

    Note: Depending on the field that was modified, you may or may not see the change on the browse screen.

24. Now that you have added and changed records in the Service Desk Ticketing system using the Power App, you want to test how the app works in deleting an existing record.

    Scroll down through the list and select the **right arrow (>)** for the record that you added at the start of this task. This displays the **Details** screen for that item.

25. To delete this record, select the **trash can** icon.

26. Once the record is deleted, the browse screen should be displayed. Scroll down through the record list to verify that the record no longer appears.

27. You should now verify that the record has been deleted from the Service Desk Requests list in the IT Services site. Select the **IT Services – Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll down through the list and verify the record no longer appears.

28. Switch back to the **App – Power Apps** tab in your browser. The app should still be running in preview mode; if not, press **F5** on your keyboard to run the app.

29. You should still be on the browse screen for the app. To stop running the app and return to preview mode, select the **X** in the circle that appears in the upper right corner of the screen.

30. If a **Did you know?** dialog box appears, select the **Don't show me this again** check box and then select **Ok**.

31. Now that you have validated that the Power App can successfully add, edit, and delete records in the Service Desk Requests list in the IT Services site, you want to save the app so that your users can access it.

You should be back in preview mode in the **Power Apps Studio**. In the menu bar at the top of the page, select **File** on the top left side of the screen

32. On the **Settings** page, you should enter the following information:

    - Name - **Service Request Ticketing App**

    - Icon – You can optionally change the icon for your app by scrolling down through the list of preformatted icons and selecting a different one

    - Background color – You can change the background color for the icon by scrolling down though the available background color samples and selecting a new one

    - Description – **This app maintains service request tickets in Adatum's new Service Request Ticketing system**

33. In the left-hand navigation pane (to the left of the Settings pane), select **Save.**

34. In the **Save as** window that appears, select the **Save** button that appears at the bottom of the screen.

35. On the **Service Request Ticketing** app page, select the **Share** button so that you can share this app with the IT Consultant.

36. On the **Share Service Request Ticketing app** window, in the **Enter a name, email address, or Everyone** field, enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix for **your fellow student that was assigned to you by your instructor**). Select the **MOD Administrator (guest)** user account that is displayed in the user list below this field, and then select **Share**.

37. Close the **Share Service Request Ticketing app** window by selecting the **X** in the upper right corner of the window.

38. This returns you to the **Apps > Service Request Ticketing app** window. Close this tab in your browser.

39. You should have two Power Apps tabs open in your browser – the **Power Apps** tab that displays Power Apps Studio, and the **Service Request Ticketing app** tab that displays the browse screen for the new app you just created.

    Leave both tabs open in your browser as they will be used in the next task.

27.1.1 Task 3 – Review the Power App Studio

Now that Holly Dickson has built her first Power App and has used it to successfully manage data in Adatum's new Service Request Ticketing system, she wants to spend more time familiarizing herself with the contents of Power Apps Studio. In your role as Holly, you will use this task to review Power Apps Studio so that you can learn how the app works and view all the details behind each component.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. In you Microsoft Edge browser, the **Service Request Ticketing app** tab should still be open from the prior task; if not, repeat the steps from the prior task to create a new app using the **Service Desk Requests** list in SharePoint as your data source. Once you reach the point of previewing the app, then stop and move on to the next step in this task.

3. In **Power Apps Studio**, the navigation pane on the left side of the screen shows the **Tree view** for the screens contained in the application. There are two menu tabs in this Tree view – **Screens** and **Components**. The **Screens** tab is underlined, indicating that it's the tab currently being displayed (it is displayed by default). Select the **X** that appears to the right of **Tree View** to close this pane.

4. By closing the Tree View pane, you see a vertical ribbon on the left-side of the screen that displays multiple icons. Hover your mouse over each icon to see what they are called.

   Select the first icon (the three horizontal lines) to expand the pane to show the names of the remaining icons. If you select this same icon again, the pane contracts and only shows the icons.

5. Select the second icon, which is the **Tree view**. This opens the **Tree view** pane that you started with. We will return to this pane later, so for now, select the **X** to close it.

6. Select the third icon, the plus (+) sign, to display the **Insert** pane. The **Insert** pane displays different components that can be added to an app. Scroll down through the list of components to familiarize yourself with what can be added, but do not add anything at this time. When you are done, select the **X** to close the pane.

7. Select the fourth icon, the database icon, to display the **Data** pane. This pane displays the source used in the current app, which is the **Service Desk Requests** list. From here you can add additional data sources to your app if you desire (you will not do so for the Service Request Ticketing app). Select the **X** to close the pane.

8. Select the fifth icon to display the **Media** pane. This pane enables you to upload images, video, and audio files to use in your app. Select the **X** to close the pane.

9. Select the final icon to display the **Advanced Tools** pane. This pane enables you to monitor activity within your app and write tests to validate the app. Select the **X** to close this pane.

10. Select the **Tree view** icon to re-open the **Tree view** pane.

11. From the **Tree view**, notice on the bottom bar on the screen that **BrowseScreen1** is currently being displayed. This object is also highlighted in the **Tree view**, where it's currently expanded. Select **BrowseScreen1** in the **Tree view** to contract this tree.

    Note that there are three screen objects available for this app – the browse screen (**BrowseScreen1**), the detail screen (**DetailScreen1**), and the edit screen (**EditScreen1**).

    Note: If necessary, use the slider bar at the bottom of the screen to enlarge the image to make it more legible.

    Select the **right arrow (>)** next to **BrowseScreen1** to expand it again.

12. Under the **BrowseScreen1** tree, select **BrowseGallery1** and notice what gets selected on the app screen - the area in the app where the data records are displayed; this area is known as the Gallery. Also notice the pane that is displayed on the right-hand side of the screen. This is known as the **Properties** pane. It displays the properties of the item that you selected in the **Tree view**.

13. In the **Tree view** pane, under the **BrowseGallery1** tree, select **IconNewItem1**. Notice how the **plus sign (+)** icon on the top right corner of the app screen gets selected. The app screen is displayed on what is called the **canvas pane**.

    Important: Every component viewed in your app screen has a corresponding component in the **Tree view**.

14. Select different components under the **BrowseGallery1** tree and notice which portion of the app screen is selected. Also review the available properties for the selected item in the **Properties pane**.

15. In the **Tree view**, select the **Components** tab that appears to the right of the **Screens** tab. This tab is used for adding additional components; that is, you can add an item from the **Insert** pane or connect to another data source. You can import components and export components as well. This is an advanced feature that is beyond the scope of this course.

16. Select the **Screens** tab to return to the app screen.

17. Leave this tab open in your browser for the next task.

27.1.2   Task 4 - Customize the Power App

The app that Holly created in the earlier task is known as a canvas app. It was developed entirely by PowerApps based on a data source, which in this case was the Service Desk Requests list in SharePoint. One of the benefits of canvas apps is that they are customizable, even if they were not built from a blank canvas. In this section, you will make a small customization to the existing app.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. In your Microsoft Edge browser, the **Service Request Ticketing app** tab should still be open from the prior task. If the **Tree view** pane is not open, then open it now.

3. In the **Tree view** pane, under the **Screens** tab, expand **BrowseScreen1** (if necessary) and select **BrowseGallery1**.

4. In the **Properties** pane, notice that on the top of the window it says **Gallery.** This indicates the type of component and underneath it shows the name given to the gallery component, **BrowseGallery1**.

5. In the **Properties** pane, locate the **Layout** property for the gallery, which displays **Title, subtitle, and body.** Select the drop-down arrow for this field to see the available layout values in a **List** window. If you wanted to, this is where you would modify the layout of the gallery. Select the **Title, subtitle, and body** layout option to return to the **BrowseGallery1** window.

6. On the **Properties** pane, locate the **Fields** property (it appears above the Layout property). Select **Edit**, which appears to the right of the **Fields** property. A new **Data** window opens which shows the fields from the SharePoint list that are mapped to the Body, Subtitle, and Title fields that appear for each record displayed in the browse screen.

7. Holly has decided to customize the browse screen to change the **Body1** field so that it maps to the **Assigned To** column of the SharePoint list. Select the drop-down arrow for the **Body1** field and scroll up and select **Assign To**.

8. In the **Data** window, notice two changes - the value in **Body1** is now **Assign To**, and a **Display value** field has appeared below the **Assign To** value. Select the drop-down arrow for the **Display value** field, and in the menu list, select **DisplayName**.

   Notice how the records displayed in the gallery have been updated to reflect the **Assign To** field.

9. Close the **Data** window by selecting the **X** in the upper right corner.

10. Holly now wants to customize the browse screen to change the **Title1** field so that it maps to the **Issue Title** column of the SharePoint list. Select the drop-down arrow for the **Title1** field, select **Issue Title**, and then close the **Data** window.

11. You are now ready to save your changes to the app. Select **File** from the top menu bar of the PowerApps screen, and then select **Save** from the navigation pane that appears on the left side of the screen. In the body of the screen, in the **Service Request Ticketing app** window, select the **Save** button.

12. In the **Service Request Ticketing app** window, it should display a message indicating that all changes were saved. However, to propagate the saved changes to the live version of the app, you must publish the app. To do so, select the **Publish** button.

13. In the **Publish** dialog box that appears, select **Publish this version**. The changes are saved and published so the next time you preview the app, it will include the update.

14. Now that the changes have been saved and published, you can share the app with additional users if you wish. However, at the time you created the app in the previous task, you only shared it with the IT Consultant's **MOD Administrator** account. Since you don't want to share it with any other users at this time, you will just ignore this **Share** option.

15. In your Edge browser, close **all** the Power Apps-related tabs that are open. In this next exercise, you will open a new Power Apps session to start fresh.

27.1.3 Task 5 - Add the Ticketing System app to Microsoft Teams

In your role as Holly Dickson, you have created the new Service Desk Ticketing system in SharePoint, and you just created a Power App that can access this system and maintain service desk tickets within it. At this point, you thought your work with the new ticketing system was done.

However, the IT Consultant has just informed Holly that there's another way in which she can make the ticketing system available to Adatum's users. By adding the Power App that she just created to Microsoft Teams, Adatum's employees can work directly from Teams to access the app and submit their service request tickets. Holly is very excited to test this out. In your role as Holly Dickson, you will perform this task to add the new Power App to Microsoft Teams.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. You will first verify whether Teams is configured to allow the use of PowerApps.

   In your Edge browser, select the **Microsoft 365 admin center** tab if it's still open; if not, open the **Office 365 home** page and select the **Admin** icon. If required, log into Microsoft 365 as holly@xxxxxZZZZZZ.

onmicosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and a password of **Pa55w.rd**.

3. In the **Microsoft 365 admin center**, select the **...Show all** option in the navigation pane to display the admin centers, and then select **Teams**.

4. In the **Microsoft Teams admin center**, in the left-hand navigation pane, select **Teams Apps**, and then select **Manage apps**.

5. In the **Manage apps** window, since there are so many apps in the apps list, you will use the **Search** feature to quickly locate PowerApps. Enter **Power Apps** in the **Search by name** field. This field is on the right-side of the menu bar, above the row of column headings.

6. In the list of apps, select **Power Apps.**

7. In the **Power Apps** window, verify the **App status** is set to **Allowed**. If this is set to **Blocked**, then select this toggle switch to change it to **Allowed**.

8. You will now enable the Power App for your Service Desk Ticketing system within Teams.

   Switch to **LON-CL1**, where you should already be logged in as the **Administrator** with a password of **Pa55w.rd**.

9. Since Holly created the Service Request Ticketing system app, you must be logged into Teams as Holly to add this Power App to Teams.

   If the **Teams** app is not open on your taskbar, then enter **Teams** in the **Search** box on the taskbar, select **Microsoft Teams** from the menu, and if prompted, sign in as holly@xxxxxZZZZZZ.onmicosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

   If you are not prompted to sign in, then check to see who the Teams apps is signed in under. If the user icon is **Holly Dickson**, then skip to the next step; otherwise, select the user icon and in the menu, select **Sign out**, sign back in as holly@xxxxxZZZZZZ.onmicosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**, and then select **OK** if a **Stay signed in to all your apps** window appears.

10. If an **Enjoy the team and the teamwork!** window appears, select **Let's go!**.

    In the **Teams** window, towards the bottom of the left-hand navigation pane, select **Apps**.

11. In the **Apps** window, enter **Power Apps** in the **Search all apps** field at the top of the left-hand navigation column.

12. In the search results in the body of the window, select **Power Apps**.

13. In the **PowerApps** window, select the drop-down arrow to the right of the **Add** button. In the drop-down menu that appears, select **Add to a team**.

14. In the **Set up Power Apps for a team** window, select inside the **Search** field; this will display the **General** channel for Adatum Corporation. Select **General.**

15. The system will display **Adatum Corporation > General** in the **Search** field. Select the **Set up a tab** button at the bottom of the page.

16. After processing for a short period, a **Choose from existing apps** window will appear. The **Service Request Ticketing app** that Holly just finished creating should appear in the list. Select this app.

    Important: Note the message that appears at the bottom of the window: **Make sure your team can use this app. If you're its owner, share access.** Since you shared this app with the IT Consultant's MOD Administrator account at the time you published the app, you do not need to share it with anyone else at this time for the purpose of this lab. However, in a real-world scenario, once you were ready to make an app available to other users within the organization, you would need to share the app with them either at the time you published it, or at this point in the process when adding the app to Teams.

17. Select **Save.**

18. This opens the **General** channel. Note how a new tab was created at the top of the page for the **Service Request Ticketing app**, which is currently selected. The app is running in the window, which enables you to access and maintain service tickets in the **Service Desk Requests** list in SharePoint.

19. Since the Power App was shared with your IT Consultant's MOD Administrator account, you can test this feature by either requesting that your fellow student log into Teams in his or her VM environment using LON-CL1, or testing it yourself by signing out of Teams as Holly and logging back in as the IT Consultant's MOD Administrator account (**admin@xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is **your fellow student's tenant prefix that was assigned to you by your instructor**).

In either case, once Microsoft Teams is open, select **Teams** from the navigation pane. The **General** channel will appear by default, so select the **Service Request Ticketing app** tab at the top of the form to initiate the Power App within Microsoft Teams.

27.1.4 Task 6 – Run the app from a mobile device (optional)

This task, which is strictly optional, provides instruction on how to run an app from a mobile device. While you can test this out if you would like with the **Service Request Ticketing app**, these instructions are simply provided for your benefit for future use with any Power Apps that you wish to use.

1. To run the app from your mobile device, download and install **Power Apps** from the **App Store** or **Google Play** onto an iPhone, iPad, or Android device.

2. The app will be available in the list of published Power Apps. Open the app and sign-in as **holly@ xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix that was provided by your lab hosting provider). Enter your tenant password as the Password.

3. Tap on the **Service Request Ticketing app** to run it.

4. The first time you open PowerApps on your mobile device you may see some instructions on how to close the app (swipe left on an iPhone).

5. To pin the app, close out of the app (swipe left on an iPhone), select the **ellipses** icon, select **Pin to Home** from the menu, and then follow the instructions on the screen for your particular device.

Congratulations! You have created a Power App from a SharePoint data source, which in this case was the new Service Desk Ticketing system that you earlier created in SharePoint.

28   Proceed to Lab 3 - Exercise 7

29   Module 4 - Lab 3 - Exercise 7 - Create a Power App from scratch

In the previous exercise, you used Power Apps to automatically build a canvas app from the SharePoint data source. In this exercise you will build a similar app from scratch, using the same SharePoint list as the data source. The purpose of this exercise is for you to learn how to build an app from scratch.

In the prior lab exercise when Power Apps created the app for the Service Desk Ticketing system, it automatically created the following screens used in the app – the browse screen, the detail screen, and the edit screen. When you create a canvas app from scratch, you will manually create each of these screens instead:

- **Screen 1 – Browse screen.** The Browse screen will display the list of records from your SharePoint list, but it will only display a limited set of fields from each record.

- **Screen 2 – Detail screen.** The Detail screen will display all the fields for one specific record. If you select a record on the Browse screen, the detailed information for that record will be displayed on the Detail screen. This screen will also enable you to delete the record that you are viewing.

- **Screen 3 – Edit screen.** The Edit screen has data entry fields for adding information for a new record or changing information for an existing record.

When you initially create these screens, you will just create their forms with their basic structure. Once the screens are in place, you will then add trigger mechanisms to these screens to add, view, edit, and delete records in your SharePoint list.

29.0.1 Task 1: Create the Browse screen for your Power App

In your role as Holly Dickson, you will begin the process of creating a canvas app from scratch by building the app's Browse screen.

1. Switch to LON-DC1, where you should still be logged in as **ADATUM\Administrator** and password **Pa55w.rd**; if not, then do so now.

2. In your Microsoft Edge browser, open a new tab and enter the following URL in the address bar: **https://make.powerapps.com**

3. This will open the **Power Apps studio**. On the main body of the **Home** page, under the **Make your own app** section, select **Canvas app from blank**.

4. On the **Canvas app from blank** window that appears, enter a name for your app (anything that you want) in the **App name** field, and in the **Format** section, select the **Phone** option.

5. Select the **Create** button at the bottom of the window. If a **Welcome to Power Apps studio** dialog box appears, select **Skip**.

6. In the **Power Apps** studio, notice how in the **Tree view** pane, none of the browse, detail, or edit screens appear under the **Screens** tab. Those screens were automatically created when you created an app from an existing data source, as you did in the prior lab exercise. But when creating a canvas app from scratch, as you are doing here, you must manually create those screens.

    Screen1 is the only screen in the Tree view pane since it is the name of the blank screen that appears on the canvas. By default, the font size on the screen is so small (20%) that it is difficult to read. Use the slider to increase the font size. While the text on the screen says **Add an item from the insert pane or connect to data**, do not select either of these options at this time. You will eventually configure the properties of this screen from the **Insert** pane, but for now, let's begin by renaming this app screen.

    In the **Tree view** pane, select the **ellipses** icon that appears to the right of **Screen1**. In the menu that appears, select **Rename**, and then enter **BrowseScreen1** as the new screen name (this will keep the screen name consistent with the naming convention that is used when Power Apps automatically creates screens for an app).

7. Now you will access the **Insert** pane to configure screen properties. On the menu bar at the top of the Power Apps Studio screen, select **Insert**.

8. On the **Insert ribbon** that appears below the menu bar, select **Gallery**, and in the menu that appears, select **Vertical**.

9. On the canvas pane, you will see the vertical gallery and a **Select a data source** window. Note that in the **Tree view** pane, the default name of the vertical gallery you just added is **Gallery1.** Gallery1 represents the list of records that will be displayed in BrowseScreen1 from your data source. Since you have yet to define a data source, you can see that it simply fills in sample records. Once you select your data source, you will see the actual records from your data source in the gallery of the Browse screen.

    In the **Select a data source** window, enter **Share** (short for SharePoint) in the **Search** field. This will display a list of data sources starting with **Share**. In the list, select **SharePoint**. Alternatively, you could select the down arrow next to **Connectors** and select **SharePoint**.

    Important: If you happened to click somewhere else on the screen before you performed the prior step of entering **Share** in the Search box, the **Select a data source** window will disappear. **Do not worry!** You will simply perform this step using the **Properties pane**. First, in the **Tree view** pane, select **Gallery1** if it is not already selected. In the **Gallery1 Properties pane** on the right, in the **Data source** field, select the drop-down arrow. In the window that appears, select **Connectors** and then select **SharePoint**.

10. In the **SharePoint** window that appears, select the **SharePoint** connection that is listed (this displays the administrator's email associated with the SharePoint connection).

11. A **Connect to a SharePoint site** window opens on the right side of the screen that lists the available SharePoint sites at the bottom of the window. Select **IT services** – **https://xxxxxZZZZZZ.sharepoint.com/sites/** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

12. In the **Choose a list** window, you must select the SharePoint list for this site that you want to use as the data source for this app. Select the check box next **Service Desk Requests** and then select **Connect** on the bottom of the screen.

Note: As soon as Power Apps connects to the **IT Services** site and the **Service Desk Requests** list, note how the gallery is updated with the items from the list.

13. On the canvas for **BrowseScreen1**, with **Gallery1** still selected in the **Tree view** pane, reduce the screen size on the slider to about 40% so that you can see more of the screen. Scroll from the top to the bottom of the screen and notice how the Gallery's border starts at the very top of **BrowseScreen1** and goes a little past the middle of the screen.

    Since Holly wants to add a couple of controls to the top of this screen (an **Add** icon and a **Refresh** icon), you need to make room at the top of the screen for these controls. Therefore, you need to move the Gallery down to provide space at the top of the screen for the controls.

    To do this, first scroll down to the bottom of the screen (so that you can see the bottom of **BrowseScreen1**). Then hold your mouse over the middle circle in the bottom border line of the Gallery; this will change your mouse icon to an up and down arrow. With your left mouse button held down, drag the bottom border of the gallery to the very bottom of **BrowseScreen1**.

    Next, scroll to the very top of **BrowseScreen1** and repeat this process with the top border line of the gallery. However, in this case, move it down to about where the top of the second sample record begins. This leaves basically the height of the first sample record space to insert the two control icons later in this exercise.

    Note: Depending on where your slider is set, you may not be able to see the blank space that you just created at the top of the screen, even after scrolling to the top. If this occurs, set your slider to 100% to see the top of the screen. You will need to set it to 100% in later tasks when adding your controls. For now, you can set the slider to a smaller percentage if you wish to see more records in the Gallery.

14. On the **Gallery1 Properties pane** on the right side of the screen, select the **down arrow** next to the **Layout** property and select the option labeled **Title, subtitle, and body**. Notice how the gallery is updated based on this selection.

15. Holly now wants to change which fields that are displayed in the gallery. In the **Properties pane**, select **Edit** that appears to the right of the **Fields** property. A new **Data** window opens which shows the **Body**, **Subtitle**, and **Title** fields; these are the three fields you selected for the **Layout** property in the prior step. For each field, you can select which field from the SharePoint list you want displayed in that field. Power Apps selects a default SharePoint field for each, but you can change them to display whatever fields that you want.

    Holly has decided to customize the browse screen to change the **Body1** field so that it maps to the **Assigned To** column of the SharePoint list. Select the drop-down arrow for the **Body1** field. Note how the field is selected in the Gallery image. Select the drop-down arrow again for the **Body1** field to display the list of available fields. Scroll to the top of the list and select **Assign To**.

16. In the **Data** window, notice two changes - the value in **Body1** is now **Assign To**, and a **Display value** field has appeared below the **Assign To** value. Select the drop-down arrow for the **Display value** field, and in the menu list, select **DisplayName**.

17. Notice how the records displayed in the gallery have been updated to reflect the **Assign To** field.

18. Repeat this process by changing the **Subtitle** field to **Issue Status** and the **Title** field to **Issue Title**.

19. Close the **Data** window by selecting the **X** in the upper right corner.

20. You have now finished creating the browse screen for your app. While you can continue creating the Detail and Edit screens for your app, as a best practice it is recommended that you save each screen in the app as you complete it.

    Select **File** from the top menu bar of the PowerApps screen, and then select **Save** from the navigation pane that appears on the left side of the screen. Since the app has yet to be saved, a **Save as** screen appears. You want to accept the default setting on this screen that will save it to Power Apps in the cloud, and you want to keep the name that you previously assigned; therefore, simply select the **Save** button.

21. In the **<app name>** window, it should display a message indicating that all changes were saved. Since you have not finished creating all the necessary screens for your app, you do **NOT** want to publish it at

this point in time. **Do NOT** select the **Publish** button. Instead, at the top of the navigation pane, select the back arrow to return to the Power Apps studio.

22. You have now finished creating the browse screen for your new app. Leave the Power Apps tabs open in your browser and proceed to the next task to create the Detail screen.

29.0.2   Task 2 – Create the Detail screen for your Power App

Holly is now ready to create screen #2 for her app, which is the Detail screen. In a Power App, the browse screen displays a summary of the items from the selected data source, which in this case is the Service Desk Requests list for the IT Services site. If the user selects an item from this browse list, the app will display all the fields for that item within a Detail screen. You will create the Detail screen for your app in this task.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the Browse screen for your app in the prior task. The tab should be displaying the **Insert** tab from the menu bar; if not, select it now.

   In the **Insert ribbon** that appears below the menu bar, select **New Screen**. In the menu of available screen types that appears, select **Blank**. This opens a new blank screen on the canvas pane that is titled **Screen2**.

2. In the **Tree view** pane under the **Screens** tab, select the **ellipses** next to **Screen2**, select the **Rename** option from the menu that appears, and then enter **DetailScreen1** in the name field.

3. Verify that **DetailScreen1** is selected in the **Tree view** pane (if not, select it now). On the **Insert ribbon**, select **Forms**, and in the menu that appears, select **Display**. The Detail form will display the fields for an individual record, but it will not allow you to edit the record (Note – in a later task, you will create the Edit screen, and for that screen, you will select Edit as the form type rather than Display).

   Note: In the **Tree view** pane, this action has added a display form titled **FormViewer1** under **DetailScreen**1.

4. If necessary, in the screen canvas in the middle of the page, scroll to the top to see the top of the form box. The form box is inserted by default at the top of page. Since you want to leave the top of the page open to add additional controls, you should move the empty form box down on the page to make space available at the top.

   To move the form box, hover your cursor over the circle that appears in the middle of the top border line for the form box. Note how the cursor image changes to an up and down arrow. At this point, hold the left mouse key and move the box down to the center of the page. Leave some space on the top of the page to add some additional controls later in this task.

   Note: You can repeat this process by grabbing the bottom border line of the form box and dragging it to the bottom of the form to provide additional space to display the fields for a given record (to avoid having to scroll through the fields if at all possible).

5. With the **FormViewer1** display form still selected, go to the **Properties pane** and select the down arrow in the **Data source** field. In the pop-up window that appears, select **Service Desk Requests**.

   In the canvas in the middle of the page, the form should immediately update to reflect the column headers from this SharePoint list; however, no data values are displayed at this point.

6. When a user selects an item on the Browse screen, the fields associated with that item will be displayed in this Detail screen. To accomplish that, you must associate the properties of the item selected from the SharePoint list with the fields in this Detail screen. You will do this by configuring a function property that is associated with each item in the form.

   Below the **Insert ribbon** is a **Function property bar**. The field on the left side of the function currently displays **Data Source.** Select the down arrow that appears in this field. A menu appears that displays the properties for the display form that you just added. Select **Item**.

7. Notice how the **function box** that appears to the right of the **Item** field is blank. The item property for the display form represents the record from the data source that will be displayed. In this case we want the item to be the record the user selects from the gallery in **BrowseScreen1**. If you will recall, the gallery of records displayed in BrowseScreen1 is titled **Gallery1**.

In the function box, enter **Gallery1.Selected** and then press Enter.

Note: By entering this function, the display form in the canvas will populate with values that map to the columns from the SharePoint list. The display form will select the values from the first record in the SharePoint list. In practice, when a user selects a record from the list of items in **BrowseScreen1**, the details of that record will be displayed in this **DetailScreen1** screen.

8. In the **Tree view** pane, under **DetailsScreen1**, you will see the control named **FormViewer1** (this is the display form). Select the arrow (**>**) that appears to the left of this control to expand it. Notice all the **Data Cards** that appear under this form control; these represent the columns of the SharePoint list record that are displayed in **DetailsScreen1**.

   Note: These Data Card controls in the **Tree view** pane enable you to customize the fields displayed on this screen. For example, you remove any of the fields if you do not want to see them in this Detail screen by selecting the Data Card in the Tree view pane, selecting the ellipsis icon that appears to the right of it, and them selecting the **Delete** option. Because Holly wants to display all the SharePoint fields, do not remove any of them from the Detail screen.

   However, for this app, Holly wants to rearrange the order of the fields. Select the **FormViewer1** control (if necessary) in the **Tree view** pane, then go to the **Properties pane** and select **Edit Fields**, which appears next to the **Fields** property.

9. In the **Fields** window that appears, the fields appear in the order in which they will be displayed in this form. Holly has decided to move the **Customer** field up so that it appears after the **Date** field.

   Hover your cursor over the **Customer** field and note how an **ellipses** icon appears to the right of the field. Select this **ellipses** icon. In the menu that appears, select **Move up**. As you do this, notice how the **Customer** field moves up one spot in the list, above the **Location** field.

   Repeat this process until the **Customer** field is below the **Date** field.

10. Close the **Fields** window by selecting the **X** in the upper right corner.

11. You have now finished creating the detail screen for your app, which you want to save before making any additional changes.

   Repeat the process that you learned earlier to save the file and then return to the Power App studio. Do **NOT** publish the app yet as you still have additional changes to make.

12. Leave the Power Apps tabs open in your browser and proceed to the next task to assign a trigger action to the Detail screen.

29.0.3   Task 3: Assign a trigger action to view the Detail screen

In the prior task, you created the DetailScreen1 that will be used to display the detailed record information for an item that the user selects in BrowseScreen1. However, this will do you no good until you configure a trigger action within the app that instructs it to display DetailScreen1 when the user selects a record in BrowseScreen1. You must also configure a trigger action that enables you to return from DetailScreen1 back to BrowseScreen1. You will create both trigger actions in this task.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the detail screen for your app.

   In the **Tree view** pane, it should currently be displaying **FormViewer1**. Scroll up in the list until **BrowseScreen1** appears. If **BrowseScreen1** is not expanded, then select the arrow (**>**) that appears to the left of it to expand it now.

2. Under **BrowseScreen1**, select **Gallery1**.

3. Below the **Insert ribbon** is the function property that you configured in the prior task for **FormViewer1** (it displays **Items** in the field on the left and the function to the right of it). In this task, you will replace these values with a function property specific to Gallery1. This property will provide the trigger action to display the Detail screen when the user selects an item in the Browse screen.

In the prior step you selected **Gallery1** (under **BrowseScreen1)**. If you recall, Gallery1 represents the summarized list of items in the Browse screen. You will now configure this function property to create the trigger action that controls what to do when an item within Gallery1 is selected on the Browse screen.

In the **Function property bar**, select the down-arrow for the field on the left side of the function, and in the menu that appears, scroll down and select **OnSelect**.

4. On the formula input box, enter **Navigate(DetailScreen1)** and then press Enter.

5. You have now created the trigger action so that when a user selects a record from the gallery in BrowseScreen1, the app will display the details for that record in DetailScreen1.

   To test whether you have properly configured this trigger action, **press F5** to go into Preview mode. Select any record in the gallery and Power Apps should display the record details in DetailsScreen1. Close Preview mode by selecting the **X** in the upper right corner of the screen.

6. If necessary, select **Gallery1** under **BrowseScreen1** in the Tree view. Review the list of records displayed in the gallery in BrowseScreen1. On the right side of each record is a right arrow ($>$), which is referred to as the **NextArrow** control. If a user selects this arrow, it will also display the details for the record. So if you are wondering why you configured an **OnSelect** trigger action to display the details of a record when you can simply select the **NextArrow** control, the answer is that the trigger action simply provides another option for displaying the record details.

   The difference between the two options is that using the **Next Arrow** control requires the user to specifically select the arrow key to navigate to the details screen. By configuring the **OnSelect** trigger action as you did, the user can instead select anywhere on the record.

7. Now that you can navigate from BrowseScreen1 to DetailsScreen1, you need to make sure you have a way to navigate back to BrowseScreen1. You will do this by adding a **Back** arrow to **DetailScreen1**, and then you will configure the arrow so that when it's selected, it returns **BrowseScreen1**.

   In the **Tree view pane**, scroll down and select **DetailsScreen1.**

8. In the **Insert ribbon**, select **Icons**. In the menu that appears, scroll down and select **Back.**

   Note: In the **DetailScreen1** image, notice how the **Back arrow** icon (the $<$ inside the circle) appears on the screen.

9. In the **Tree view** pane, notice how under **DetailScreen1** it now displays the **Icon1** control. The **Icon1** control is selected in the **Tree view** pane because when you inserted the **Back arrow** in the earlier step, Power Apps studio inserted the icon in DetailScreen1 and left it selected.

10. After reviewing the Detail screen, you decide that you want to make two cosmetic changes to the **Back arrow** icon – you want to change its color, and you want to display a tool tip that says "Back" when you hover your mouse over it.

    Since the **Icon1** control is selected in the **Tree view** pane (if not, select it now), the **Properties** pane displays the properties for this control. In the **Properties** pane, scroll down to the **Color** field, to the right of which are two boxes. The first box displays a capital **"A"** with a colored line below it. This line is currently black.

    To change the color of the **Back arrow** icon, select this field and then select the color of your choice from the color menu that appears. Note that you can select different colors to see which one you prefer. Each time you select a color, the color of the **Back arrow** icon in the **DetailScreen1** image changes to that selection.

    Once you have selected the color that you want to use, press the **Esc** key on your keyboard to close the color menu. This will keep **Icon1** selected (if you select anywhere else, it will also close the color menu, but **Icon1** will be unselected and you will have to select it again to add a tool tip to the icon).

    Scroll further down the **Properties pane** until you get to the **Tooltip** property. Select the **Tooltip** box, enter **Back**, and press Enter.

    Note: Hovering your mouse over the **Back arrow** icon on DetailScreen1 does not display the tool tip. You will test this out when you finish all other edits in this task and use Preview mode to test the changes

that you made.

11. You now need to configure this **Back arrow** icon so that when the user selects it, **BrowseScreen1** is returned. In the **Tree view** pane, select the **Icon1** control under **DetailScreen1** if it's not already selected.

    In the **Function property bar**, the field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Back arrow** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

12. On the formula input box, enter **Navigate(BrowseScreen1)** and then press Enter.

    You have now created the trigger action so that when a user selects the **Back arrow** icon in **DetailScreen1**, the app will return to **BrowseScreen1**.

13. To test whether you have properly configured this trigger action, **press F5** to go into Preview mode. The record that was selected in the gallery will be displayed in **DetailScreen1**.

    You should begin by hovering your mouse over the **Back arrow** icon, which should display the **Back** tool tip. Select the **Back arrow** icon, which should return you to **BrowseScreen1**.

    Close Preview mode by selecting the **X** in the upper right corner of the screen.

14. You have now finished creating the trigger mechanism for the Detail screen for your app, which you want to save before making any additional changes.

    Repeat the process that you learned earlier to save the file and then return to the Power App studio. Do **NOT** publish the app yet as you still have additional changes to make.

15. Leave the Power Apps tabs open in your browser and proceed to the next task to create the Edit screen.

29.0.4 Task 4 - Create the Edit screen for your Power App

Holly is now ready to create screen #3 for her app, which is the Edit screen. This screen will enable users to add new Service tickets to the SharePoint list and edit and delete existing ones. You will create the Edit screen for your app in this task.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the trigger actions for the Detail screen in the prior task. The tab should be displaying the **Insert** tab from the menu bar; if not, select it now.

    In the **Insert ribbon** that appears below the menu bar, select the drop-down arrow key next to **New Screen**. In the menu of available screen types that appear, select **Blank**. This opens a new blank screen on the canvas pane that is titled **Screen1**.

2. On the **Tree view** pane, select the **ellipses** next to **Screen1** and rename it to **EditScreen1**.

3. **EditScreen1** should be selected in the **Tree view** pane (if not, select it now). On the **Insert ribbon**, select **Forms**, and in the menu that appears, select **Edit**.

    Note: In the **Tree view** pane, this action has added an edit form titled **Form1** under **EditScreen1.**

4. If necessary, in the screen canvas in the middle of the page, scroll to the top to see the top of the form box. The form box is inserted by default at the top of page. Since you want to leave the top of the page open to add additional controls, you should move the empty form box down on the page to make space available at the top.

    To move the form box, hover your cursor over the circle that appears in the middle of the top border line for the form box. Note how the cursor image changes to an up and down arrow. At this point, hold the left mouse key and move the box down to the center of the page. Leave some space on the top of the page to add some additional controls later in this task.

5. With the **Form1** edit form still selected, go to the **Properties pane** and select the down arrow in the **Data source** field. In the pop-up window that appears, select **Service Desk Requests**.

In the canvas in the middle of the page, the form should immediately update to display data entry boxes that are associated with each of the column headers from this SharePoint list.

6. Below the **Insert ribbon** is the **Function property bar**. The field on the left side of the function currently displays **DataSource.** Select the down arrow that appears in this field. A menu appears that displays the properties for the edit form that you just added. Select **Item**.

7. Notice how the **function input box** that appears to the right of the **Item** field is blank. The item property for the edit form represents the record that will be added to the data source that will be displayed.

   In the function box, enter **Gallery1.Selected** and then press Enter.

   Note: By entering this function, the edit form in the canvas will populate with values that map to the last selected item in the gallery of BrowseScreen1.

8. You have now finished creating the edit screen for your app, which you want to save before making any additional changes.

   Repeat the process that you learned earlier to save the file and then return to the Power App studio. Do **NOT** publish the app yet as you still have additional changes to make.

9. Leave the Power Apps tabs open in your browser and proceed to the next task to assign a trigger action to the Detail screen.

29.0.5 Task 5 - Assign trigger actions to create a new entry

The Edit screen that you created in the prior task provides the form needed to enter the data for a new entry. However, while the form is ready for entering data, you must create several trigger mechanisms to process this form; three of the triggers are associated with specific icons being added to screens, and the another facilitates automatic navigation between screens:

- **Add icon -** You must add a trigger mechanism to display the Edit screen when you are on the Browse screen and you select an **Add** icon to add a new record.

- **Save icon -** You must add a trigger mechanism to submit the data for processing once the user has completed entering data in the Edit screen and selects a **Save** icon.

- **Navigation -** You must add a trigger mechanism to navigate away from the Edit screen and back to the prior screen that initiated the Edit screen (either the Browse screen when adding a record and the Detail screen when editing a record) if the data has been successfully submitted.

- **Cancel icon -** You must add a trigger mechanism to navigate away from the Edit screen and back to the prior screen if the user selects a **Cancel** icon.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the Edit screen in the prior task. The tab should be displaying the **Insert** tab from the menu bar; if not, select it now.

2. In the **Tree view** pane, select **BrowseScreen1**.

3. In the earlier task when you first created **BrowseScreen1**, the Gallery's border went to the very top of the screen. Since you knew you would be adding controls to the screen later on, you moved the Gallery's top border down to provide enough space to add these controls.

   The first control you want to add is an **Add** icon for creating a new item. Scroll to the top of **BrowseScreen1** so that you can see the top of the screen with the blank space you configured for the controls.

   Note: Depending on where your slider is set, you may not be able to see the blank space at the top of the screen, even after scrolling to the top. If this occurs, set your slider to 100% to see the blank space at the top of **BrowseScreen1.**

   On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Add**. Notice how the **Plus sign (+)** icon shows up on the screen, and in the **Tree view** pane, **Icon2** appears below **BrowseScreen1**.

4. You now must associate a trigger mechanism to this **Plus sign (+)** icon so that when the user selects it, **EditScreen1** will be returned.

Below the **Insert ribbon** is the **Function property bar**. The field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Plus sign (+) sign** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

5. In the function box, enter **NewForm(Form1); Navigate(EditScreen1)** and then press Enter.

   This function actually encapsulates two separate actions:

   - **NewForm(Form1)** - changes the form mode to New to enable the entry of a new record in **Form1**, which is the name of the edit form under **EditScreen1**.

   - **Navigate(EditScreen1)** – navigates the user to the screen (EditScreen1) which contains the edit form (Form1).

6. Now that the **Plus sign (+)** icon has been configured, you decide that you want to make some cosmetic changes to it. First, you decide that you want to change the location of the icon from the top left corner of **BrowseScreen1** to the top right. To do this, select the border of the **Plus sign (+)** icon (so that an image of crossed arrows appears) and drag it across to the right corner.

7. Next, you want to change the color of the icon and assign it a tool tip.

   If the **Plus sign (+)** icon is not selected, then click on it now (this will select **Icon2** under **BrowseScreen1** in the **Tree view** pane and display the **Properties pane** for Icon2 on the right side of the page).

   Repeat the processes that you learned earlier to select a color and to add a tooltip for this icon. Choose whichever color you wish and enter **Create new item** for the tooltip.

8. You must now enter a second trigger mechanism that will be associated with a **Save** icon. This icon and trigger mechanism will ensure that the data the user enters in the Edit screen can get saved to the data source, which for this app is the **Service Desk Requests** SharePoint list.

   In the **Tree view** pane, select **EditScreen1**.

9. On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Check**. Notice how the **check mark** icon shows up on the screen, and in the **Tree view** pane, **Icon3** appears below **EditScreen1**.

10. Now that you have added the **check mark** icon to **EditScreen1**, you must associate a trigger mechanism to the check mark so that the data is submitted when the **check mark** icon is selected. In the **Tree view** pane, the **Icon3** control should be selected; if not, then do so now.

    In the **Function property bar**, the field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **check mark** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

11. In the function box, enter **SubmitForm(Form1)** and then press Enter.

12. You have just associated a trigger mechanism to submit the data in the edit form (**Form1**) for processing when the check mark icon is selected. You must now create another trigger mechanism to navigate away from **Form1** and back to the prior screen once the data has been successfully submitted. **This is a navigation trigger; there is no icon associated with it.**

    In the **Tree view** pane, under **EditScreen1**, select **Form1**.

13. In the **Function property bar**, the field on the left side of the function currently displays **Item**. Select the down arrow for this field and select **OnSuccess** from the menu.

14. In the function box, enter **Back()** and then press Enter.

15. You must now add one final trigger mechanism to the data entry form (Form1), which is the ability to cancel the data entry operation and return to the prior screen. This trigger will be associated with a **Cancel** icon.

    In the **Tree view** pane, under **EditScreen1**, select **Form1** if it's not already selected.

16. On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Cancel**. Notice how the **"X"** (Cancel) icon shows up on the screen, and in the **Tree view** pane, **Icon4** appears below **EditScreen1**.

17. You notice that the "X" (Cancel) icon is partially placed over the check mark icon in the upper left corner of the screen. To fix this, you want to move the "X" icon to the upper right corner of the form. To do this, select the border of the "X" icon (so that an image of crossed arrows appears) and drag it across to the right corner. You will also need to drag it up a bit so that it's on the same line as the check mark icon.

18. Now that you have added the **Cancel** icon to **EditScreen1**, you must associate a trigger mechanism to the icon so that EditScreen1 is reset and the user is returned back to the most recently processed screen when the "X" icon is selected. In the **Tree view** pane, the **Icon4** control should be selected; if not, then do so now.

    In the **Function property bar**, the field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Cancel** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

19. In the function box, enter **ResetForm(Form1); Back()**.

    This function actually encapsulates two separate actions:

    - **ResetForm(Form1)** - resets **Form1**, which is the name of the edit form under **EditScreen1**.
    - **Back()** - takes the user back to the most recently displayed screen.

20. After reviewing the Edit form, you decide that you want to change the colors of the two icons that you just added to **EditScreen1**, and you want to add a tooltip for each as well. With prior icons, you selected the color of your choice. However, for these two icons, the IT Consultant has suggested to Holly that she use two specific colors – green for the check mark and red for the "X" icon.

    Since you cannot remember which control in the **Tree view** pane is associated with each icon, on the canvas for **EditScreen1**, select the **check mark** icon. In the **Tree view** pane, you notice this selects **Icon3** under **EditScreen1**. The **Properties pane** on the right also displays the properties for this icon.

    Repeat the processes that you learned earlier to select a color for this icon and to add a tool tip. At the bottom of the Color menu under **Standard colors**, select the **Green (RGBA 54, 176, 75, 1)** box. For the **Tooltip**, enter **Save**.

    Next, select the "X" icon on the **EditScreen1** canvas, which selects **Icon4** under **EditScreen1** in the **Tree view** pane. The **Properties pane** on the right also displays the properties for this icon.

    Repeat the processes for selecting a color and adding a tool tip for this icon. At the bottom of the Color menu under **Standard colors**, select the **Red (RGBA 255, 0, 0, 1)** box. For the **Tooltip**, enter **Cancel**.

21. To test whether you have properly configured these trigger actions, select **BrowseScreen1** in the **Tree view** pane and then press **F5** on your keyboard to run the app in Preview mode.

22. Because you selected **BrowseScreen1** prior to pressing **F5**, the browse screen will appear, and it will display the existing records from the **Service Desk Requests** list. You want to add a new record, so select the **Plus (+) sign** icon in the upper right corner of the form. This should display the edit form (**EditScreen1**).

23. Populate the form with the following data:

    - Issue Status – **Active**
    - Date – **June**
    - Issue Title (and Title, if you created the list using PowerShell) – **Test record**
    - Description – **Testing trigger actions**
    - Location – **Home Office**
    - Customer – enter **Megan** and select **Megan Bowen** from the list

- Assign To – leave this field blank

24. To test the **Save** functionality, begin by hovering your mouse over the green **check mark** icon, which should display the tool tip of **Save.** Once you have verified the tool tip displays properly, select the **check mark** icon to submit the form.

25. Since the **Assign To** field is a required field, an error message should be displayed at the top of the screen indicating that one or more fields have errors. Scroll down through the form and note the specific error message below the **Assign To** field.

    In the **Assign To** field, enter **Allan** in the field and then select **Allan Deyoung** from the list.

26. Select the **check mark** icon to submit the form.

27. This time, all the data should have been successfully processed, the record should have been added to the **Service Desk Requests** list, and **BrowseScreen1** should be returned.

28. You should now verify that the record has been added to the **Service Desk Requests** list in the **IT Services** site.

    Select the **IT Services – Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll down through the list and verify the record that you entered appears in the list.

29. Switch back to the **<app name> - Saved (Unpublished) – Power Apps** tab in your browser. You should still be on the browse screen for the app (**BrowseScreen1**) and it should still be running in Preview mode.

30. Select the **Plus (+) sign** icon to display the edit form.

31. To test the **Cancel** functionality, begin by hovering your mouse over the red **X** icon, which should display the tool tip of **Cancel**. Once you have verified the tool tip displays properly, select the **X** icon; this should return you to the **BrowseScreen1.**

32. To stop running the app in Preview mode, select the **X** in the circle that appears in the upper right corner of the screen.

33. You have now finished creating the trigger mechanisms for adding and canceling records in your app, which you want to save before making any additional changes.

    Repeat the process that you learned earlier to save the file and then return to the Power App studio. Do **NOT** publish the app yet as you still have additional changes to make.

34. Leave the Power Apps tabs open in your browser and proceed to the next task to add Edit and Delete functionality to the Edit screen.

29.0.6 Task 6 - Assign trigger actions to edit and delete a record

Now that Holly has created the ability to add a new record into the SharePoint list, she wants to be able to edit and delete existing records as well. In this task, you will create the triggers needed to edit and delete a record in your app.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the Edit screen in the prior task. The tab should be displaying the **Insert** tab from the menu bar; if not, select it now.

2. In the **Tree view** pane, select **DetailScreen1**.

3. If necessary, scroll to the top of the canvas so that you can see the top of the **DetailScreen1** form. On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Edit**. Notice how the **Edit (Pencil)** icon shows up on the screen, and in the **Tree view** pane, **Icon5** appears below **DetailScreen1**.

4. You notice that the **Pencil** icon is partially placed over the **Back arrow** icon in the upper left corner of the screen. To fix this, you want to move the Pencil icon to the upper right corner of the form. However, since you also want to add a Delete icon to this screen in a later step, you do NOT want to move the Pencil icon into the far right corner. In the right corner of the form, you want to display both the Edit icon and the Delete icon, where the Edit icon appears to the left of the Delete icon. Therefore, you want to move the Pencil icon to the right, but still leave room to the right of it for the Delete icon.

To do this, select the border of the Pencil icon (so that an image of crossed arrows appears) and drag it across to the right corner, making sure you leave enough room to the right of it for the Delete icon. You will also need to drag it up a bit so that it's on the same line as the **Back arrow** icon.

5. Now that you have added the **Edit** icon to **EditScreen1**, you must associate a trigger mechanism to it so that EditScreen1 is displayed when the **Edit** icon is selected. In the **Tree view** pane, the **Icon5** control should be selected; if not, then do so now.

   In the **Function property bar**, the field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Edit** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

6. In the function box, enter **EditForm(Form1); Navigate(EditScreen1)** and then press Enter.

   This function actually encapsulates two separate actions:

   - **EditForm(Form1)** - changes the form mode to Edit to enable updates to an existing record, where **Form1** is the name of the edit form under **EditScreen1**.

   - **Navigate(EditScreen1)** – navigates the user to the screen (**EditScreen1**) containing the edit form.

7. You now want to add another icon to **DetailScreen1** that enables you to delete a record. In the **Tree view** pane, select **DetailScreen1**.

8. If necessary, scroll to the top of the canvas so that you can see the top of the **DetailScreen1** form. On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Trash**. Notice how the **Trash (trash can)** icon shows up on the screen, and in the **Tree view** pane, **Icon6** appears below **DetailScreen1**.

9. You notice that the **Trash** icon is partially placed over the **Back arrow** icon in the upper left corner of the screen. To fix this, you want to move the **Trash** icon to the upper right corner of the form and to the right of the **Pencil** icon. To do this, select the border of the Trash icon (so that an image of crossed arrows appears) and drag it across to the right corner, to the right of the **Pencil** icon. You will also need to drag it up a bit so that it's on the same line as the **Pencil** icon.

   Note: If you did not leave enough room for the Trash icon when you originally added the Pencil icon, you may need to move the Pencil icon to allow enough room for the Trash icon.

10. Now that you have added the **Trash** icon to **DetailScreen1**, you must associate a trigger mechanism to it so that the selected record is deleted from the SharePoint list when the **Trash** icon is selected. In the **Tree view** pane, the **Icon6** control should be selected; if not, then do so now.

    In the **Function property bar**, the field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Edit** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

11. In the function box, enter **Remove('Service Desk Requests', Gallery1.Selected); If(IsEmpty(Errors('Service Desk Requests', Gallery1.Selected)), Back())** and then press Enter (copy and paste this function if your VM environment provides a copy and paste feature; this will ensure that you do not enter a typo).

    This function actually encapsulates two separate actions:

    - **Remove('Service Desk Requests', Gallery1.Selected)** - removes from the SharePoint list titled Service Desk Requests the entry that was selected from the gallery in BrowseScreen1.

    - **If(IsEmpty(Errors('Service Desk Requests', Gallery1.Selected)), Back())** - checks for the existence of errors when editing the SharePoint list. Errors can occur for many reasons, including network outages, inadequate permissions, and edit conflicts. If there are no errors (the error table is empty) then the app will go back to the most recently displayed screen. The "If" statement does not include any action if there are errors in the error table; however, PowerApps will, by default, display a message.

12. After reviewing the Detail form, you decide that you want to change the colors of each icon and display a tool tip when you hover your mouse over them.

Since you cannot remember which control in the **Tree view** pane is associated with each icon, on the canvas for **DetailScreen1**, select the **Pencil** icon. In the **Tree view** pane, you notice this highlights **Icon5** under **DetailScreen1**. The **Properties pane** on the right also displays the properties for this icon.

Repeat the processes that you learned earlier to select a color and to add a tooltip for this icon. Choose whichever color you wish and enter **Edit** for the tooltip.

Next, select the **Trash** icon on the canvas. In the **Tree view** pane, you notice this highlights **Icon6** under **DetailScreen1**. The **Properties pane** on the right also displays the properties for this icon.

Repeat the processes to select a color and add a tooltip for this icon. Choose whichever color you wish and enter **Delete** for the tooltip.

13. To test whether you have properly configured these trigger actions, select **BrowseScreen1** in the **Tree view** pane and then press **F5** on your keyboard to run the app in Preview mode. **BrowseScreen1** will display the existing records from the **Service Desk Requests** list.

14. You must first select a record from the gallery. Find a record, and then select the > icon. This should display the record in the Detail screen.

15. To test the Edit functionality, begin by hovering your mouse over the **Pencil** icon, which should display the **Edit** tool tip. Select the **Pencil** icon, which should display the Edit form with the data for the selected record pre-filled in the fields.

    Make a change to any of the fields in this record (**Hint:** change something that will be easy to find in the SharePoint list and BrowseScreen1, such as changing the value of the **Issue Status** to **EDIT TEST**). Then hover your mouse over the green check mark icon, which should display the **Save** tool tip. Select the **check mark** icon to save your changes.

    If the change was successful, the Detail screen should return. You should see your changes in the information displayed on the screen.

16. You should now verify that the record has been changed in the **Service Desk Requests** list in the **IT Services** site.

    Select the **IT Services − Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll down through the list and verify the record that you entered appears in the list.

17. Switch back to the **<app name> - Saved (Unpublished) – Power Apps** tab in your browser. You should still be on the Detail screen for the app (**DetailScreen1**) and it should still be running in Preview mode (if not, select **DetailScreen1** in the **Tree view** pane and then press F5 on the keyboard). The record that you just changed should still be displayed.

18. To test the Delete functionality, you should delete the record that you just changed, which will make it easy to determine that the record no longer exists in the SharePoint list.

    Begin by hovering your mouse over the **Trash** icon, which should display the **Delete** tool tip. Select the **Trash** icon, which should delete the record from the SharePoint list and then take you back to the browse screen (**BrowseScreen1**).

19. You should now verify that the record has been deleted from the **Service Desk Requests** list in the **IT Services** site.

    Select the **IT Services − Service Desk Requests** tab in your browser, and then select the **Refresh** icon on the left side of the address bar. Scroll down through the list and verify the record that you deleted does not appear in the list.

20. Switch back to the **<app name> - Saved (Unpublished) – Power Apps** tab in your browser. You should still be on the Browse screen for the app (**BrowseScreen1**) and it should still be running in Preview mode. You should see that the deleted record no longer appears in this list as well.

    To stop running the app in Preview mode, select the **X** in the circle that appears in the upper right corner of the screen.

21. You have now finished creating the trigger mechanisms for editing and deleting records in your app, which you want to save before making any additional changes.

    Repeat the process that you learned earlier to save the file and then return to the Power App studio. Do **NOT** publish the app yet as you still have additional changes to make.

22. Leave the Power Apps tabs open in your browser and proceed to the next task to add a control that refreshes the connected data source.

29.0.7   Task 7 - Assign trigger to refresh the connected data source

With the three screens for her app now in place, Holly wants to add one more control to the Browse screen. This control will refresh the connected data source (the SharePoint list) to ensure that what the user sees in the Browse screen is always current.

1. You should still have the **<app name> - Power Apps** tab open in your browser from when you finished creating the Edit and Delete triggers in the prior task. The tab should be displaying the **Insert** tab from the menu bar; if not, select it now.

2. In the **Tree view** pane, select **BrowseScreen1**.

3. In the earlier task when you first created **BrowseScreen1**, the Gallery's border went to the very top of the screen. Since you knew you would be adding controls to the screen later on, you moved the Gallery's top border down to provide enough space at the top of the screen to add these controls. You then added the **plus sign (Add)** icon for creating a new record, and you moved it to the top right corner of the screen. You now want to add the **Reload** icon and move it to the left of the **Add** icon.

    Scroll to the top of **BrowseScreen1** so that you can see the top of the screen with the **Add** icon.

    Note: Depending on where your slider is set, you may not be able to see the space at the top of the screen that contains the **Add** icon, even after scrolling to the top. If this occurs, set your slider to 100% to see the **Add** icon at the top of **BrowseScreen1.**

    On the **Insert ribbon**, select **Icons**, and in the menu that appears, select **Reload**. Notice how the **Reload** icon shows up on the screen, and in the **Tree view** pane, **Icon7** appears below **BrowseScreen1**.

4. You now must associate a trigger mechanism to this **Reload** icon so that when the user selects it, the list of data that is displayed in the Gallery will be refreshed.

    Below the **Insert ribbon** is the **Function property bar**. The field on the left side of the function currently displays **OnSelect.** While this value is left over from the prior task, it's also the trigger action that you want to associate with this **Reload** icon. If **OnSelect** is not displayed in this field, select the drop-down arrow and select it from the menu.

5. In the function box, enter **Refresh('Service Desk Requests')** and then press Enter.

Now that the **Reload** icon has been configured, you decide that you want to make some cosmetic changes to it. First, you decide that you want to change the location of the icon from the top left corner of **BrowseScreen1** to the left of the **Add** icon. To do this, select the border of the **Reload** icon (so that an image of crossed arrows appears) and drag it across to so that it's to the left of the **Add** icon.

6. Next, you want to change the color of this icon and assign it a tool tip.

    If the **Reload** icon is not selected on the canvas for **BrowseScreen1**, then select it now. This will select **Icon7** below **BrowseScreen1** in the **Tree view** pane and display the **Properties pane** for this icon.

    Repeat the processes that you learned earlier to select a color and to add a tooltip for this icon. Choose whichever color you wish and enter **Refresh list** for the tooltip.

7. To test whether you have properly configured the Reload trigger action, select **BrowseScreen1** in the **Tree view** pane and then press **F5** on your keyboard to run the app in Preview mode. **BrowseScreen1** will display the existing records from the **Service Desk Requests** list.

8. You must now add a new record into the SharePoint list. Select the **IT Services – Service Desk Requests** tab in your browser and then add a new record to the list.

9. Once you have added this record, switch back to the **<app name> - Saved (Unpublished)** – **Power Apps** tab in your browser. You should still be on the Browse screen for the app (**BrowseScreen1**), and it should still be running in Preview mode.

10. Select the **Reload** icon and then verify that the new record that you added to the **Service Desk Requests** list appears in the list of records.

    To stop running the app in Preview mode, select the **X** in the circle that appears in the upper right corner of the screen.

11. You have now finished creating the trigger mechanism for refreshing the record list in your Browse screen. This completes the process of creating a Power App from scratch, so you're ready to save your final changes and then publish the app.

    Repeat the process that you learned earlier to save the file; however, after saving the changes, you now want to select the **Publish** button. In the **Publish** dialog box that appears, select **Publish this version**.

12. Now that the final changes have been saved and the app is published, the **<app name>** window provides you with the ability to share the app with additional users. We will not be sharing this app, since you already shared the prior app that you created with the IT Consultant's MOD Administrator account.

13. In your browser, close all the Power Apps-related tabs that are open.

Congratulations! You have created a Power App from scratch that provides the ability to add, edit, delete, and view records from a data source.

30 Proceed to Lab 3 - Exercise 8

31 Module 4 - Lab 3 - Exercise 8 - Create a flow using Power Automate

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have built a new service desk ticketing system in SharePoint that consists of a team site titled **IT Services** and a SharePoint list titled **Service Desk Requests**. In your effort to implement Microsoft's Power Platform at Adatum, you then created a Power App that enables users to enter service tickets using the app rather than SharePoint, and you also added the app to Microsoft Teams so that users can access the Power App through Teams.

As part of your Power Platform pilot project, you now want to investigate how you can use Power Automate to improve your new ticketing system. After reviewing Adatum's old ticketing system, you realized that a lack of real-time communication between managers and customers (your internal users) was a key factor in its ineffectiveness. To address this issue, you have decided to build and share an automated flow within Power Automate that automatically sends an email to the MOD Administrator whenever a service request is created or modified.

31.0.1 Task 1 - Create a Power Automate Flow

To improve communication between management and internal users, Holly Dickson has decided to build and share an automated flow within Power Automate that sends an email to Adatum's MOD Administrator whenever a service request is created or modified. This task will focus on creating the flow; the next task will address how to share the flow with another manager.

1. After having completed the prior lab exercise in which you created a Power App from scratch, you should still be logged into your Domain Controller VM (LON-DC1) as **ADATUM\Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. In your Microsoft Edge browser, make sure that your new ticketing system is open in a tab. The tab should be titled **IT Services – Service Desk Requests – All Items**. If you do not have this tab open, then go to the **SharePoint admin center**, select **Active Sites**, select **IT Services** from the **Active Sites** list, select **Site contents**, and then select the **Service Desk Requests** list.

3. In your Edge browser, you want to open the Power Automate studio. Open a new tab in the browser and enter the following URL in the address bar: **https://flow.microsoft.com**

    On the **Microsoft Power Automate** screen, select **Sign in** at the top of the screen.

4. If you are not already signed in with your corporate account, you will be prompted for your credentials, in which case you should enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and a password of **Pa55w.rd**.

5. In the **Welcome to Power Automate** screen, select your **country/region** from the drop-down list and then select **Get Started**.

6. On the **Power Automate studio** screen, validate that Holly Dickson's initials (**HD**) appear in the user icon in the upper right corner of the screen. If this user icon is someone other than Holly, then select the user icon, select **Sign out**, and then sign back in as Holly (**Holly@xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and a password of **Pa55w.rd**.

7. From the left navigation pane, select **+ Create.**

8. On the **Three ways to make a flow** page, scroll down on the landing page until you see **Start from connector**, and then select **SharePoint**.

9. On the **SharePoint** page, scroll down to view SharePoint triggers and templates.

10. In the list of triggers, select **When an item is created or modified**.

11. On the **When an item is created or modified** window appears, select the drop-down arrow in the **Site address** field. A list should appear displaying the URL for the **IT Services** site that you created and published: **IT Services - https://xxxxxZZZZZZ.sharepoint.com/sites/ITServices** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). Select this site.

    Note: If you do not see the **IT Services** site in the drop-down list, then switch to the browser tab containing the **Service Desk Request** list and copy the URL. Switch back to the browser tab running the Power Automate designer tool, select **Enter custom value,** and then past the URL for the **Service Desk Request** list. However, notice how Power Automate trims the URL so that it is only the site address and does not include the name of the list. You will need to do the same here.

12. In the **List Name** field, select the **drop-down arrow**, and in the list that appears select **Service Desk Requests**.

13. Select **Show advanced options.**

14. In the **Limit Columns by View** field, select the **drop-down arrow**, and in the list that appears select **Enter custom value**. Then in the **Limit Columns by View** field, enter **Active cases by Support Agent**.
    Note: The purpose of this field is to help avoid column threshold issues. The **All Items** view, which is the default view for this SharePoint list, displays all the available columns. On the other hand, the **Active Cases by Support Agent** view uses only a partial set of columns.

15. Select the **+ New step** button.

16. The next screen in the Power Automate designer tool requires that you choose an action to be performed when an item is created or modified. Holly wants to send an email to Adatum's MOD Administrator.

    In the **Search connectors and actions** field at the top of the screen (below **Choose an action**), type in **Outlook**. Under the **All** tab that appears below this Search field, select **Office 365 Outlook**. This will display a list of all the actions available for the Office 365 Outlook connector.

17. From the list of actions, scroll down and select **Send an email (V2).**

18. This opens an email form. Since Holly wants to send an email to Adatum's MOD Administrator, enter the following information in this email:

    - **To** - enter **MOD** in the field. A list of user accounts starting with MOD will appear. This list should include two MOD Administrator accounts – one for Adatum's MOD Administrator, and one for the IT Consultant's MOD Administrator. Select **Adatum's MOD Administrator**, whose tenant suffix ID was provided to you by your lab hosting provider. Do **NOT** select the account whose tenant suffix ID is your fellow student's tenant ID that was assigned to you by your instructor.

      (**Note:** There is hypertext located at the bottom right of the flow tray that reads **Add dynamic content**. You can use this to input data directly from the ticket item)

    - **Subject** – Select inside the **Subject** field; this will display a list of parameters that you can choose from to display in the **Subject** line of the email. This list includes various connectors as well as

each field from the **Active Cases** view that you selected earlier. Scroll down in the list and select **Issue Title.** Note that when you make this selection, **Issue Title** appears in the **Subject** field. The subject line of the email will be the actual **Issue Title** for the item that was added or edited in the SharePoint list.

Note: You can add additional parameters to the subject line; however, for this lab you will only select the **Issue Title**.

While Holly only wants to display the **Issue Title** in the Subject line, she does want to add additional text to the subject line of the email. In the **Subject** field, place the cursor in front of the SharePoint parameter **Issue Title** (click on the left hand edge of the SharePoint icon to see a cursor marker appear in the field; if you select in the blank space in front of the SharePoint icon, it will not insert the cursor marker) and enter **New or edited Service Request:** (leave a space after the colon).

- **Body** – Below the menu bar in the **Body** field is the message area that displays the following message: **Specify the body of the email.** Select this message, which displays a list of available SharePoint parameters. You can create the body of the email by adding one or more of these parameters along with text that you enter.

  Feel free to enter anything that you wish, but here is an example that you could enter that includes text and two parameters from the list (the value of the **Customer** and **Assign To** fields in the ticket that was added or edited):

  A service request ticket submitted by <Customer DisplayName> and assigned to <Assign To DisplayName> was added or edited.

  Note: If you use this example, make sure you add a space before and after the selected parameters (**Customer DisplayName** and **Assign To DisplayName).**

19. At the bottom of the email form, select **Show advanced options**. Scroll to the bottom of the list, select the **Importance** field, and in the list that appears, select **Normal**.

20. At the bottom of the page, select **Save**. Scroll up to the top of the screen, where in the top-left corner, it displays the name that Power Automate assigned to this flow: **When an item is created or modified -> Send an email (V2)**.

    Holly wants to change this to a more user-friendly name. To rename the flow, select this flow name, which highlights the name. Enter **Service Request flow for new/modified tickets** and then select anywhere below the name.

21. At the top right corner of the screen (on the same row as the flow name), select **Flow checker**. In the **Flow checker** pane that appears, there should be zero errors and zero warnings.

    Note: If an error or warning occurs, select the drop-down arrow to the left of the Error or Warning line to display the specific issues.

    Select the **X** in the top right corner of the **Flow Checker** pane to close it.

22. At the top right corner of the screen, select **Test.** On the **Test Flow** pane that appears, select the **I'll preform the trigger action** option, and then select **Save & Test**. Leave this browser tab open.

    Note: If at any time you accidentally close this tab or navigate away from this page, select **My flows** in the left-hand navigation pane, select this flow from the list of flows, and then in the menu bar that appears at the top of the page for this flow, select **Edit**. That will return you to this window where you can run the **Flow Checker** and run a **Test**.

23. In your browser, select the **IT Services - Service Desk Requests – All Items** tab.

24. In the **Service Desk Requests** list, create a new ticket with the following information:

    - Issue Status – **Active**

    - Date – enter the current month

    - Issue Title – **Power Automate Flow test**

- Description – **Testing the flow**

- Customer – enter **Megan**, then select **Megan Bowen** from the list

- Assign To – enter **Allan**, then select **Allan Deyoung** from the list
  Note: Alternatively, you could open the Power App that you created in the earlier exercise and create an entry to the Service Desk Requests SharePoint list. You could open a new browser tab and enter the following URL to access the app in Power Apps studio: **https://make.powerapps.com**

25. After you create the entry on the SharePoint list, switch back to the browser tab containing the flow (the tab name will have changed to **Run History | Power Automate**).

26. On the top of the screen, you should hopefully see a message indicating **Your flow ran successfully**, and next to each step in the flow you will see **green check marks**. Keep this tab open.

27. To verify whether the flow sent an email to the **MOD Administrator**, you should check the user's Inbox in Outlook to see whether an email was received.

    Switch to **LON-CL1**.

28. On **LON-CL1**, in your Edge browser, you should be logged in as Holly Dickson. Select Holly's user icon in the upper right corner of the screen, and in the **My account** pane, select **Sign out.**

    Close Edge and all the open tabs to clear your cache, then select the **Edge** icon on the taskbar to start a new browser session.

29. In your Edge browser, enter the following URL in the address bar: **https://portal.office.com**

30. In the **Pick an account** window, select the **MOD Administrator** account for your tenant. Verify the username is **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

31. In the **Enter password** window, enter the tenant password provided by your lab hosting provider and select **Sign in**.

32. On the **Office 365 Home** page, select the **Outlook** icon from the column of app icons on the left side of the screen. This will open the **Inbox** for the **MOD Administrator**. If a **Welcome** window appears, then close it now.

33. The **Inbox** should include an email from **Holly Dickson** with a subject line that starts with: **New or edited Service Request**. Select this email to open it.

    Note: It may take a few minutes for the email to show up in the MOD Administrator's inbox. If need be, skip to step 36 and check back on the email at the end of this task.

34. After opening the email, verify the full subject line is: **New or edited Service Request: <Issue Title from the record that you created>**. Also verify that the body of the email message is correct, and that if you included any parameters in the message (such as the Customer and Assign To values), that they are correct as well.

35. Switch back to **LON-DC1**.

36. On **LON-DC1**, select the **Run History | Power Automate** tab in your browser (if necessary).

37. In **Power Automate studio**, in the left-hand navigation pane, select **My flows**.

38. In the **Flows** window, select the flow that you just created from the list of your flows.

39. Review the information in the window for this flow. Scroll down to the bottom of the window and in the **Runs** group, you will see each of the times this flow ran. You should see the run that occurred for the record that you just created in the **Service Desk Requests** list. The status of the run should be **Succeeded**, which indicates the email was sent to the MOD Administrator.
    In addition, review the menu options that appear in the menu bar at the top of the page. You will not make any changes, but for future reference, you would select **Edit** if you wish to change anything in the flow. From the **Edit** form, you can run **Flow Checker** and **Test,** just as you did earlier when you first created the flow.

40. Leave all the tabs open in your browser for the next task.

Congratulations! You have successfully created an automated flow in Power Automate that adds another level of communication in Adatum's Service Request Ticketing system.

31.0.2 Task 2 – Assign an additional owner to the flow

In this task you will add an additional owner to the Power Automate flow that you just created. Generally, it is a good practice to designate additional owners to a flow, just as you would for a SharePoint site. This ensures that any issue can be addressed, and the flow can continue to run if the primary owner has changed roles or left the company. For the flow that Holly just created for her pilot project, she wants to add Allan Deyoung as an additional owner.

1. After having completed the prior task in which you created a flow in Power Automate, you should still be logged into LON-DC1 as **ADATUM\Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. You should still have the browser tab open to the **Flows > Service Request Flow for new/modified tickets** window. If not, then repeat the steps you performed in the prior task to get to this tab (from **Power Automate studio**, select **My flows**, then select the flow you just created).

3. On the menu bar, select **Share**.

4. In the **Owners** section, in the **Add a user or group as owner** field, enter **Allan**. In the user list that appears, select **Allan Deyoung**.

5. In the **Connections Used** window that appears, read the information and then select **OK.** Note that Allan (or anyone you add as an owner) will have full access to all connections in the flow and the content within the connected accounts.

6. This will return you to the **Share** screen for the flow, and it will display Allan and Holly as owners of the flow. Select the **left arrow** that appears next the flow name at the top of the screen; this will return you to the detail screen for this flow.

   Note: On the details screen, Holly will appear as the lone owner on the left-hand side of the screen, below the flow name. This owner represents the original owner of the flow. However, in the Owners section on the bottom right side of the screen, you will see both Holly and Allan as owners of the flow.

7. On the left-hand navigation pane, select **My flows**.

8. In the **Flows** window, notice that the **Cloud flows** tab is selected by default. Also notice the message that appears in the middle of the screen indicating **You don't have any flows**. Do not worry! Since you have shared ownership of the flow with another user or group, the flow is now considered a shared flow.

9. In the **Flows** window, select the **Shared with me** tab.

10. In the **Shared with me** tab, hover your mouse over the name of the flow and select the **vertical ellipses (More commands)** icon that appears to the right of the flow name. In the menu that appears, review the options that are available. Select the **Esc** button on your keyboard to close the menu (or select anywhere on the screen).

11. Leave all the tabs open in your browser for the next task.

32 Proceed to Lab 3 - Exercise 9

33 Module 4 - Lab 3 - Exercise 9 - Create a DLP Policy using Power Automate

For security reasons, administrators oftentimes want to ensure that certain data is kept protected. Power Platform allows you to create data loss prevention policies that define which connectors can share specific business data. For example, you may not want business data that is stored in SharePoint to be automatically published to its Twitter feed by a Power Automate flow.

Power Platform uses data groups as a simple way to categorize connectors within a DLP policy. The three data groups available are the Business data group, the Non-Business data group, and the Blocked data group.

A good way to categorize connectors is to place them in groups based on the business-centered or personal-use-centered services they connect to in the context of your organization. Connectors that host business-use data should be classified as Business, and connectors that host personal-use data should be classified as Non-Business. Any connectors that you want to restrict usage of across one or more environments should be classified as Blocked.

When a new policy is created, by default all connectors are placed in the Non-Business group. From there they can be moved to Business or Blocked based on your preference. For a flow to run, all its connectors must be in one group or the other. If your flow has connectors in both groups, then the flow will automatically be suspended and will not run. Since all connectors are assigned by default to the **Non-business** group, if you want to include any data in your flow, you must add all the connectors used in the flow into the Business data only group.

In this exercise, you will create a DLP policy that uses two connectors - a SharePoint connector and an Office 365 Outlook connector. For the flow to work that uses this DLP policy, you must move both connectors to the Business data group.

33.0.1 Task 1: Create a data loss prevention policy

In this task, Holly wants to create a data lost prevention policy for the flows that she plans to create as part of her pilot project. In this task, she will initially add the **SharePoint** connector to **Business** group. She will then see how this affects the flow that she just created.

1. After having completed the prior exercise in which you created a flow in Power Automate and assigned to it an additional owner, you should still be logged into LON-DC1 as **ADATUM\Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. You should still have your Edge browser open to the **Microsoft Power Automate** tab, which should still be displaying the **Flows** window and the **Team flows** tab. If not, then repeat the steps you performed in the prior task to get to this tab (from **Power Automate studio**, select **My flows**, and then select the **Team flows** tab).

3. In the top right corner of the screen, select the **gear (Settings)** icon. In the **Settings** pane that appears, under the **Power Automate** section, select **Admin Center**.

4. A new tab will open in your browser that displays the **Power Platform admin center**. In the left-hand navigation pane select **Data policies**.

5. On the **Data policies** page, select the **+New Policy** button. This initiates a **New Policy** wizard, which displays the pages to be completed in the middle pane on the screen.

6. In the **Policy Name** page, enter **DLP Policy** in the **Name your policy** field and then select **Next**.

7. In the **Assign Connectors** page, the menu bar displays tabs for three groups of connectors - the **Business** connectors (there are currently no Business connectors), the **Non-business** connectors (which currently includes over 400 connectors; this is also the default tab displayed), and the **Blocked** connectors (which also contains no connectors).

   In the list of **Non-business** connectors, you want to select the connector for SharePoint.

   The quickest way to select the SharePoint connector is to use the **Search connectors** field that appears to the right of the menu bar. Enter **share** in this field. This will filter the list of **Non-business** connectors and only show those with **share** in the connector name. This will save you from having to scroll down through hundreds of **Non-business** connectors to those whose name starts with **share**.

   Before you select the SharePoint connector, note how nothing appears above the **Assign connectors** heading at the top of the page. Now, in the list of filtered **Non-business** connectors, select the **Share-Point** connector. Once you selected the SharePoint connector, notice how the **Move to Business** option now appears at the top of the page.

8. Since Adatum wants the connector for this policy to share data with connectors in other groups, you must move the SharePoint connector from the **Non-business** group to the **Business** group.

   To do so, select the **Move to Business** option at the top of the page. Once the connector has been moved, note how the **Business** tab now displays **(1)** next to it (indicating there is now one Business connector), and how the number of **Non-business** connectors is now reduced by 1. Select the **Business** tab to see the SharePoint connector. Select **Next**.

9. On the **Scope** page, you must define the environment to which the new policy will apply. Select the **Add all environments** option and then select **Next**.

10. On the **Review** page, review all the settings that you previously assigned to the new policy. If any setting needs to be changed, select the **Edit** option for that setting. If all settings are correct, select the **Create policy** button.

11. On the **Data policies** page, you should now see in the list of policies the new **DLP Policy** that you just created.

    Important: You have created a data policy that has one of the two connectors used in your flow (Share-Point) in the **Business** group. However, Holly has forgotten that she actually has two connectors in her flow; the second connector is **Office 365 Outlook**, which manages the email that is automatically created and sent by the flow. This connector remains in the **Non-business** group.

    In practice, you would not be able to implement this policy as you need both connectors used by the flow in the same group. If both connectors are not in the same group, the policy will be automatically suspended. Continue on to see how connectors in both groups impact the flow.

12. In your Edge browser, select the **View your flow owners | Power Automate** tab to return to the **Flows** window that displays your flow in the **Shared with me** tab.

13. Select the **Service Request Flow for new/modified tickets**, which displays the detail information about the selected flow.

    Note: The Status of the flow is **On**. Eventually, once the policy propagates through the system, the status will change from **On** to **Suspended**.

    Important: It can take several minutes for the policy to propagate; in testing, it has been found to take approximately 5 minutes. After that time, select the **Refresh** icon that appears to the left of the address bar. In the **Details** section, notice the **Status** of the flow, which should change from **On** to **Suspended**.

    Do NOT proceed to the next step until the **Status** of the flow has changed to **Suspended**. You may need to refresh the window a few times until you see this status change.

14. Once the flow has been suspended, select **Edit** in the menu bar at the top of the page.

15. In the window that is returned, you will see the actions for your flow. Select **Save**.

    A **Flow Checker** pane appears on the right-side of the screen. Each of the two connectors used in this flow have been flagged as violating Adatum's DLP policy, since both connectors are not in the same group. Close the **Flow checker** pane.

    Important: Since this flow was already created at the time the policy was established, Power Automate automatically suspended the flow, which, in effect, turned the flow **Off**. If you subsequently create a new entry or modify an existing entry in the SharePoint list after the flow has been suspended, the flow will not run.

16. At the top of the page, to the left of the flow name, select the left arrow to return to the Detail page for the flow.

17. In the heading at the top of the page, **Flow > Service Request Flow for new/modified tickets**, select **Flow** to return to the list of **Shared with me** flows.

18. Leave your Edge browser and all its tabs open for the next task.

33.0.2   Task 2: Edit your data loss prevention policy

Although you created the DLP policy using the Power Platform admin center, the policy applies to all applications and flows in the Adatum Corporation environment. As such, the policy would apply for any Power App that uses these connections.

Now that Holly has seen what happens when she creates a DLP policy that only includes the SharePoint connector, she realizes that she needs to update the policy to include both Outlook and SharePoint in the group of **Business** connectors. While this will allow her flow to work, it will also prevent any future flow or app from running if it uses SharePoint, Outlook, and any other connector, since the additional connector is not in the **Business** group. For example, if Holly creates a second flow that includes SharePoint, Outlook, and Twitter, this first flow would still work, but the second flow would not since Twitter is not included in the **Business** group for this policy.

In your role as Holly, you will update this DLP policy to include Outlook as an additional connector in the **Business** group.

1. You should still be logged into LON-DC1 as **ADATUM\Administrator** and a password of **Pa55w.rd**; if not, then do so now.

2. You should still have your Edge browser open to the **Edit your flow | Power Automate** tab, which should still be displaying the **Flows** window and the **Shared with me** tab.

   In your browser, select the **Power Platform admin center** tab, which should be displaying the **Data policies** window. If you closed this tab at the end of the prior task, then in the **Manage your flows | Microsoft Power Automate** tab, select the gear **(Settings)** icon, select **Admin center** in the **Settings** pane, and then in the **Power Platform admin center,** select **Data policies.**

3. In the **Data policies** window, note how at the top of the screen it displays the **+New Policy** option. Now select the **DLP policy** that you created in the prior task. Note how this caused the **Edit Policy** and **Delete Policy** options to appear next to the **+New Policy** option. Select **Edit Policy**.

4. You will basically repeat the same steps that you performed in the prior task when you assigned the SharePoint connector to the policy; however, this time you will assign the **Office 365 Outlook** connector.

   On the **Policy name** page, you will not change the policy name, so simply select **Next**.

5. On the **Assign Connectors** page, the **Non-business** connector group is once again displayed by default. Enter **outlook** in the **Search connectors** field. This will filter the list of **Non-business** connectors and only show those with **outlook** in the connector name. Select the **Office 365 Outlook** connector.

6. For this Office 365 Outlook connector to work with the SharePoint connector that you earlier selected, you must move the Outlook connector to the **Business** data group. To do so, select the **Move to Business** option at the top of the screen.

   Once the connector has moved, note how the **Business** tab now displays **(2)** next to it (indicating there are now two Business connectors), and how the number of **Non-business** connectors is once again reduced by 1. Select the **Business** tab to see both the SharePoint and Office 365 Outlook connectors that you have assigned to the Business group. Select **Next**.

7. On the **Scope** page, you previously selected the **Add all environments** option, so this time simply select **Next**.

8. On the **Review** page, review all the settings that you previously assigned to the new policy. If any setting needs to be changed, select the **Edit** option for that setting. If all settings are correct, select the **Update policy** button.

9. In your browser, select the **Edit your flow | Power Automate** tab to return back to the **Flows** window that displays your flow in the **Shared with me** tab. Notice that under the **Modified** column, it still indicates **Activity suspended**.

10. Select **Service Request Flow for new/modified tickets** to see the detail information about the flow.

    Important: Note that the **Status** of the flow is **Suspended**. When you first created the DLP policy, Microsoft Flow automatically changed the status of the flow from **On** to **Suspended** when you saved the policy and Flow realized that one of the data connectors for the flow was not in the policy's **Business** group. However, when you edit a policy and change the connectors in either group, Flow does not re-evaluate this change to existing flows; therefore, the status of this flow will not be automatically changed from **Suspended** to **On** even though the policy now has both **SharePoint** and **Office 365 Outlook** in the **Business** group. Instead, you will have to manually turn the flow **On**, which you will do in the next step.

    Note: If you delete a DLP policy, Flow does not re-evaluate how this policy deletion affects existing flows. Therefore, had you deleted this policy rather than modify it, your suspended flow would remain suspended, and you would have to manually turn it **On**, just as you have to do following this policy change.

11. At the top of the **Flow > Service Request Flow for new/modified tickets** window, select **Turn on** in the menu bar at the top of the page.

    This displays a message below the menu bar that says: **Your flow is off: Service Request Flow for new/modified tickets.** This message simply indicates the status of the flow prior to it being turned **On.**

12. Select the **Refresh** icon that appears to the left of the address bar. In the **Details** section, notice the **Status** of the flow, which should change from **Suspended** to **On**.

13. In your Edge browser, close the **Power Automate** and **Power Platform** tabs, but leave open the **SharePoint** tabs that are related to your **Service Desk Requests** list for the next exercise.

34 Proceed to Lab 3 - Exercise 10

35 Module 7 - Lab 4 - Exercise 1 - Prepare for Identity 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 identity is 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.

35.0.1 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 created a custom, accepted domain for Adatum titled **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx was the unique UPN name assigned to your tenant, and xxxCustomDomainxxx.xxx was the name assigned to the domain by your lab hosting provider).

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 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 the new xxxUPNxxx.xxxCustomDomainxxx.xxx 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. On your Domain Controller VM (LON-DC1), make sure you're logged in as **ADATUM\Administrator** and password **Pa55w.rd**.

2. If **Windows PowerShell** is still open, then select the **PowerShell** icon on your taskbar; otherwise, you must open **Windows PowerShell** by selecting the magnifying glass (**Search**) icon on the taskbar, typing **powershell** in the Search box that appears, right-clicking on **Windows PowerShell**, and selecting **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 your lab hosting provider's custom domain). 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 UPN @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 $_  -UserPrincipalN
```

5. You will continue using PowerShell on your Domain Controller VM in the next task.

35.0.2 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 an on-premises user account. As part of your Adatum pilot project, you are purposely breaking this identity object so that you can run the IdFix tool in the next task to see how you can fix the broken account.

1. On your Domain Controller VM (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 a problem user account. This script, which is stored in the C:\labfiles folder, will purposely create an issue with the UserPrincipalName for the user's on-premises account; this will enable you to troubleshoot this account 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 change in AD DS:

- **Klemen Sic**. Update the UserPrincipalName for Klemen to include an extra "@" character.

5. Close PowerShell.

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

In this task you will download and use the IdFix tool to fix the on-premises user account that was 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 **Microsoft Edge**, open a new tab and enter the following URL in the address bar to access the Microsoft Download Center 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. If a **Do you want to run this file?** dialog box appears, select **Run**.

6. In the **Do you want to install this application?** dialog box, select **Install**.

7. If a **Do you want to run this file?** dialog box appears, 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. In the **Klemen Sic** row, select the drop-down arrow in the **ACTION** field and select **EDIT**.

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

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

    Note: Notice the value in the **Action** column changed from **EDIT** to **COMPLETE** for this user; this indicates that IdFix updated the user object and corrected the error.

14. On the menu bar, select **Query**. In the query results, note how the Klemen Sic row no longer appears in the results, since you just fixed this object.

    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, 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.

15. Close the IdFix window.

16. Leave your Edge browser open.

35.0.4 Task 4: Prepare for Directory Synchronization

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.

36   Proceed to Lab 4 - Exercise 2

37   Module 7 - Lab 4 - Exercise 2 - Implement Identity 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 user and 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 four tasks without any delay between them so that Azure AD Connect does not automatically synchronize the changes that you make to the identity objects.

37.0.1   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 **Add multiple users**), and then in the drop-down menu, select **Directory synchronization**.

5. In the **Azure Active Directory preparation** window, select **Go to the Download center to get the Azure AD 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. This initiates the installation of the Microsoft Azure Active Directory Connect Tool.

   If a **Do you want to run this file?** dialog box appears, select **Run**.

   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.

9. 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@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **USERNAME** field, enter **Pa55w.rd** in the **PASSWORD** field, and then select **Next** (if the **Next** button is not enabled, then tab off the PASSWORD field to enable it).

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** (if the **Next** button is not enabled, then tab off the PASSWORD field to enable it).

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 (which may take several minutes) 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 **htps://portal.office.com**. Log in as **Holly@xxxxxZZZZZZ.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. Maximize the **Synchronization Service Manager on LON-DC1** window. The **Operations** tab at the top of the screen is displayed by default so that you can monitor the synchronization process, which automatically started when you selected this program.

18. Wait for the **Export** profile to complete for **xxxxxZZZZZZ.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** pane on the left, note the number of users that were added and the number that were updated.
    - In the **Export Errors** pane on the right, 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 (CN={xxxxxx...) under the **Export Errors** column that apply to the two **Data Validation** errors; this will display

these two users that were not synchronized by the Azure AD Connect tool due to these errors. Review the errors to see why these two accounts are broke.

Note: Because a synchronization had not been performed prior to this, the initial synchronization was a **Full Synchronization** (see the **Profile Name** column in the top pane). 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 on LON-DC1** window.

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.

37.0.2   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):

   - **Ashlee Pickett**
   - **Juanita Cook**
   - **Morgan Brooks**

8. Select **Check Names** and once they are all validated, 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**, select the **Research** folder, and then in the detail pane on the right, double-click on the **Manufacturing** security group.

14. In the **Manufacturing Properties** window, enter Manufacturing@adatum.com in the **E-mail** field.

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.

37.0.3   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.

37.0.4   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.

37.0.5 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@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**, and then on the **Microsoft Office Home** page, select the **Admin** icon.

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 AD to Azure AD, 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@xxxxxZZZZZZ.onmicrosoft.com**, which is the group's mailbox in Exchange Online.

   Hover your mouse over the icon in the **Sync status** column and verify that it indicates **Synced from on-premises**.

6. Select the **Manufacturing** group to open the **Manufacturing** pane.

7. In the **Manufacturing** pane, under the Manufacturing title at the top of the pane, note 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 the three users

114

that you added as members of the on-premises group (Bernardo, Dawn, and Charlie) have been synced up and are members of this cloud-based group as well. Close the **Manufacturing** pane.

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@xxxxxZZZZZZ.onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix 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.

38 Proceed to Lab 4 - Exercise 3

39 Module 7 - Lab 4 - Exercise 3 - Implement Password Management

As Holly Dickson, Adatum's Enterprise Administrator, you have been asked by Adatum's CTO to deploy Pass-through Authentication (PTA) and Azure AD Smart Lockout as a means of strengthening password management throughout the organization.

39.0.1 Task 1: Deploy Azure AD Pass-Through Authentication

Pass-through Authentication allows users to log in to cloud-based services using their on-premises passwords. All user passwords are only stored locally in the on-premises domains and never synchronized to the cloud. When a user logs in, the PTA agent takes the authentication to your on-premises environment to verify if the password is correct and then communicates the result with Azure AD.

Adatum's CTO wants to provide the company's users with a better logon experience (since PTA requires one less password to remember), as well as reduce Adatum's IT helpdesk costs because with PTA their users are less likely to forget how to sign in. While this can also be achieved by employing Password Hash Synchronization as well as Active Directory Federation Services, Adatum has chosen to test PTA in its pilot project.

1. On LON=DC1, select the **Start** button on the taskbar, and then in the **Start** menu, select the **Azure AD Connect** program group and then select **Azure AD Connect**. This will initiate the **Microsoft Azure Active Directory Connect** wizard.

2. In the **Welcome to Azure AD Connect** window, you will receive a page indicating the synchronization service scheduler is suspended until this setup wizard is closed. This is because if you start the Azure AD Connect installation wizard (which you did in an earlier task), then the scheduler is temporarily suspended. Select **Configure.**

3. On the **Additional tasks** page, select the **Change user Sign-in** task and then select **Next**.

4. On the **Connect to Azure AD** page, sign into Azure AD. The **USERNAME** field is already filled with **Holly@xxxUPNxxx.xxxCustomDomainxxx.xxx.** Enter **Pa55w.rd** in the **PASSWORD** field, select **Next** button to enable it, and then select the **Next** button again to proceed to the next page. .

5. On the **User sign-in** page, under the **Select the Sign On method** option, select **Pass-through authentication** and then select **Next**.

6. On the **Enable single sign-on** page, select **Enter credentials**.

7. In the **Forest Credentials** dialog box, enter **adatum\administrator** as the **User name** and **Pa55w.rd** as the **Password**, and then select **OK**.

8. When the credentials are verified, a check mark will appear to the right of the **Enter credentials** button. Select **Next**.

9. On the **Ready to configure** page, select **Configure**.

10. On the **Configuration complete** page, select **Exit**. Pass-Through Authentication has now been enabled.

11. To verify that Pass-Through Authentication is successfully enabled, select a new tab in your Edge browser and enter the following URL in the address bar: **https://aad.portal.azure.com**

12. This opens the **Azure Active Directory admin center**. In the left-hand navigation pane, select **Azure Active Directory**.

13. On the **Azure Active Directory admin center** page, in the left-hand navigation pane, select **All services**.

14. On the **All services** page, three groups are displayed - General, Identity, and Security. Under the **Identity** group, select **Azure Active Directory**.

15. On the **Adatum Corporation | Overview** page, in the middle navigation pane under the **Manage** section, select **Azure AD Connect**.

16. On the **Adatum Corporation | Azure AD Connect** page, in the detail pane on the right, under the **USER SIGN IN** section, verify that the status of **Pass-through authentication** is **Enabled**, and then select **Pass-through authentication**.

17. On the **Pass-through authentication** page, review the list of servers on which your pass-through authentication agents are installed.

18. Select the **X** in the upper-right corner of the **Pass-through authentication** page to close it, and then do the same to close the **Adatum Corporation | Azure AD Connect** page. You should now be back to the **All services** page in the **Azure Active Directory admin center**.

19. Leave the **Azure Active Directory admin center** open as you will use it in the next task.

39.0.2 Task 2: Deploy Azure AD Smart Lockout

Adatum's CTO has asked you to deploy Azure AD Smart Lockout, which assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get admitted into your network. Smart Lockout can recognize sign-ins coming from valid users and treat them differently than sign-ins from attackers and other unknown sources.

The CTO is anxious to implement Smart Lockout because it will lock out the attackers while letting Adatum's users continue to access their accounts and be productive. The CTO has asked you to configure Smart Lockout so that users can't use the same password more than once, and they can't use passwords that you deem too simplistic or common.

1. On LON-DC1, select the **Server Manager** icon on the taskbar if it's already open; otherwise, open it now.

2. In **Server Manager**, select **Tools** in the upper-right menu bar, and in the drop-down menu, select **Group Policy Management.**

3. Maximize the **Group Policy Management** window, if necessary.

4. You want to edit the group policy that includes your organization's account lockout policy. If necessary, in the root console tree, expand **Forest:Adatum.com**, then expand **Domains**, and then expand **Adatum.com**.

   Under **Adatum.com**, right-click on **Default Domain Policy** and then select **Edit** in the menu.

5. Maximize the **Group Policy Management Editor** window that appears.

6. In the **Default Domain Policy** tree in the left-hand pane, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Account Policies.**

7. In the **Account Policies** folder, select **Account Lockout Policy**.

8. As you can see in the right-hand pane, none of the smart lockout parameters have been defined. You are going to use the **Azure AD admin center** to assign these values.

   Select the Edge browser icon on the taskbar, which should be displaying the **All services** tab in the **Azure Active Directory admin center**.

9. In the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory**.

10. In the **Adatum Corporation | Overview** page, in the middle navigation pane under the **Manage** section, scroll down and select **Security**.

11. In the **Security | Getting started** window, in the middle pane under the **Manage** section, select **Authentication Methods**.

12. In the **Authentication methods | Authentication method policy** page, in the middle pane under the **Manage** section, select **Password protection.**

13. In the **Authentication methods | Password protection** window, in the detail pane on the right, enter the following information:

    - In the **Custom smart lockout** section:
      - **Lockout threshold:** this field indicates how many failed sign-ins are allowed on an account before its first lockout. The default is 10. For testing purposes, Adatum has requested that you set this to **3.**
      - **Lockout duration in seconds:** This is the length in seconds of each lockout. The default is 60 seconds (one minute). Adatum has requested that you change this to **90** seconds.
    - In the **Custom banned passwords** section:
      - **Enforce custom list**: select **Yes**
      - **Custom banned password list:** Enter the following values (press Enter after entering each value so that each value is on a separate line):
        * **Password01**
        * **F00tball01**
        * **Se@Hawks1**
        * **Never4get!!**

14. Select **Save** on the menu bar at the top of the page.

15. You should now test the banned password functionality. Select Holly Dickson's user icon in the upper right corner of the screen, and in the menu that appears select **Change password**.

16. A new tab will open displaying the **change password** window. Enter **Pa55w.rd** in the **Old password** field, enter **Never4get!!** in the **Create new password** and **Confirm new password** fields, and then select **submit**. Note the error message that you receive.

17. In your browser, close the **Change password** tab.

18. You should now test the lockout threshold functionality. In the **Authentication methods - Azure Active Directory admin center** tab, select Holly Dickson's user icon in the upper right corner of the screen, and in the menu that appears select **Sign out**.

19. Once you are signed out as Holly, the **Pick an account** window will appear. Select **Use another account**.

20. In the **Sign in** window, enter laura@xxxxxZZZZZZ.onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix assigned to you by your lab hosting provider), and then select **Next**.

21. On the **Enter password** window, enter any mix of letters and then select **Sign in**. Note the invalid password error message.

    Repeat this step 2 more times.

    Since you set the **Lockout threshold** to **3**, note the error message that you receive after the third attempt. Laura's account has been temporarily locked to prevent unauthorized access.

    Note: You will be prohibited from logging in as Laura until after the **90 second lockout duration** that you set earlier.

22. After 90 seconds, verify that you can log in once the lockout threshold has ended by logging in using the password **Pa55w.rd**. If your log in is successful, you should return to the Azure Active Directory admin center.

40   End of Lab 4