Contents

1 INF99X: Sample Course

- **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-101T00-Microsoft-365-Mobility-and-Security/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MS-101T00-Microsoft-365-Mobility-and-Security/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

3 Module 1 - Lab 1 - Exercise 1 - Set up your Microsoft 365 Tenant

In the labs for this course, you are taking on the role of Holly Dickson, Adatum Corporation's Enterprise Administrator. Adatum does NOT have legacy, on-premises servers; therefore, you will be implementing Microsoft 365 in a cloud-only deployment. You have deployed Microsoft 365 in a virtualized lab environment, and you have been tasked with completing a pilot project that tests the security, compliance, and device management features in Microsoft 365 as they relate to Adatum's business requirements.

You have just started the pilot project; therefore, in this first lab you will set up a personalized Microsoft 365 user account for Holly that will be used throughout all the labs in this course. This first exercise also requires that you perform several setup tasks that will initialize your trial tenant for the remaining labs in this course. You must configure your trial tenant, create a personalized Global Admin user account in Microsoft 365 for Holly, configure several test users and groups that will be used throughout the remaining labs, and turn on Information Rights Management (IRM) in SharePoint Online as well as audit logging.

3.0.1 Task 1 - Obtain Your Office 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.

1. Because this course can be offered by learning partners using any one of several authorized lab hosting providers, the actual steps involved to retrieve the tenant prefix, tenant ID, and tenant password associated with your trial 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. The information that you should write down for later use includes:

- **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.

3.0.2 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 Task 3), Holly will initially sign into Microsoft 365 as the default Microsoft 365 MOD Administrator account using the Tenant email address and password that was assigned by your lab hosting provider.

1. When you open your lab hosting provider's Virtual Machine environment, you need to begin with the Client 1 VM (LON-CL1). If your VM environment opens with one of the other machines, then switch to the LON-CL1 VM now.
2. On **LON-CL1**, 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-CL1 as the **Admin** (or Administrator) account with the password **Pa55w.rd**.
3. If you receive a **Networks** warning message asking if you want this PC to be discoverable by other PCs and devices on this network, select **Yes**.
4. On the taskbar at the bottom of the page, select the **Microsoft Edge** icon. Maximize your browser window when it opens.
5. In your browser go to the **Microsoft Office Home** page by entering the following URL in the address bar: **https://portal.office.com/**
6. In the **Sign in** dialog box, copy and paste in 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**.
7. In the **Enter password** dialog box, copy and paste in the **Tenant Password** provided by your lab hosting provider and then select **Sign in**.
8. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
9. In the top right corner of the screen, notice the initials **MA** that appear in a circle. These are the initials of the **MOD Administrator** account, which is the tenant admin account created by your lab hosting provider. If any of the other Microsoft 365 user accounts that were created by your lab hosting provider have a picture associated with the account, that picture will be displayed when the user logs in. 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.
10. If a **Get your work done with Office 365** window appears, then close it now.
11. On the **Microsoft Office Home** tab, in the column of Microsoft 365 app icons that appear on the left side of the screen, scroll down and select the **Admin** icon; 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 is displayed by default. Select the **Organization profile** tab.

14. In the **Organization profile** tab on the **Org settings** page, 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. Scroll to 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 will have to 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. After selecting the users, scroll to the bottom of the **Release preferences** pane to verify you selected the required users. Close the **Release preferences** pane once you verified these four users were selected.
24. Tn 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 the purpose of this lab, you can change any of the options or leave the default values as is. For example, you can add the logo of your company and set the background image as the default for all your users. Along with these options you can change the colors for your navigation pane, text color, icon color, and accent color. Go ahead and explore the different options for your tenant and make any changes that you wish.

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.
27. Remain logged into LON-DC1 with Microsoft Edge open to the **Microsoft 365 admin center** for the next task.

3.0.3 Task 3 - Create a Microsoft 365 Global Admin account

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.

Note: While your lab hosting provider has created a custom domain for Adatum (xxxUPNxxx.xxxCustomDomainxxx.xxx), they did not finish the setup process for the domain; in a later lab exercise, you will finish provisioning the new domain. That being said, your lab hosting provider should have left your Microsoft 365 tenant's **xxxxxZZZZZ.onmicrosoft.com** domain as the default domain for Adatum. In this task, you will begin by verifying whether this domain is listed as the default domain. If your lab hosting provider set the new custom domain as the default, you will change it to the xxxxxZZZZZZ.onmicrosoft.com domain. This has implications in that when you add a new user account (such as the one for Holly Dickson that you will add in this task) or email addresses for new groups (later in this exercise), you want the xxxxxZZZZZZ.onmicrosoft.com domain to show as the default domain for the user and groups.

1. On the LON-CL1 VM, the **Microsoft 365 admin center** should still be open in your Microsoft Edge browser from the prior lab, and you should be signed into Microsoft 365 as the **MOD Administrator**.
2. You will begin by verifying which domain is listed as the default domain for Adatum. In the **Microsoft 365 admin center**, in the left-hand navigation pane, under the **Settings** group select **Domains**.
3. On the **Domains** page, you should see the two domains created by your lab hosting provider - the **xxxxxZZZZZZ.onmicrosoft.com** domain and the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain.

   If the **xxxxxZZZZZZ.onmicrosoft.com*** domain displays **(Default)** next to the domain name, then skip to the next step as no change is needed.

   However, if the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain displays **(Default)** next to the domain name, then select the circle with the check mark to the left of the **xxxxxZZZZZZ.onmicrosoft.com** domain and then select **Set as default** on the menu bar.

In the **Set this domain as default?** dialog box that appears, select **Set as default**. In the list of domains, the **xxxxxZZZZZZ.onmicrosoft.com** domain should now display **(Default)** next to the domain name.

Note: If there is no **xxxUPNxxx.xxxCustomDomainxxx.xxx**, do not worry. It is not needed for any of the labs in this course.

4. You will now create a Microsoft 365 user account for Holly Dickson. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then select **Active users**.
5. 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.
6. In the **Active Users** window, select **Add a user** that appears on the menu bar above the list of active users, then select **Single User** from the submenu that appears.
7. In the **Set up the basics** window, enter the following information:
   - First name: **Holly**
   - Last name: **Dickson**
   - Display name: When you tab into this field, **Holly Dickson** will appear.
   - Username: **Holly**

     IMPORTANT: To the right of the **Username** field is the domain field. It should be prefilled with the **xxxxxZZZZZZ.onmicrosoft.com** cloud domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). However, if your lab hosting provider set the custom **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain as Adatum's default domain and you did not change the default domain to the **xxxxxZZZZZZ.onmicrosoft.com** domain earlier in this task, then the custom domain will appear here instead. If that happens, select the drop-down arrow in this domain field and select **xxxxxZZZZZZ.onmicrosoft.com**. You should also perform steps 2-3 to change **xxxxxZZZZZZ.onmicrosoft.com** to the default domain as this is needed in the next task.

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

     Holly@xxxxxZZZZZZ.onmicrosoft.com
   - Clear (uncheck) the **Automatically create a password** checkbox which will enable a new box for entering an administrator defined password.
   - In the new Password box that appears, enter: **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
8. Select **Next**.
9. In the **Assign product licenses** window, 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**
10. Select **Next.**
11. In the **Optional settings** window, select the drop-down arrow to the right of **Roles.**
12. In the **Roles** section, the **User (no admin center access)** option is selected by default. Select the **Admin center access** option instead. By doing so, the most commonly used Microsoft 365 administrator roles are displayed 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.

13. Select the **Global admin**, **Security admin**, and **Attack Simulation Administrator** check box and then select **Next**.
14. 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**.
15. 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 will need to select the **Reset a password** icon (the key icon that appears when you hover over Holly's account) to change her password to the correct value.
16. Remain logged into LON-CL1 with the Microsoft 365 admin center open in your browser for the next task.

3.0.4 Task 4 – Set up Microsoft 365 User Accounts and 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 the prior task, you noticed that your Microsoft 365 trial tenant came equipped with a list of active users. As Holly Dickson, Adatum's Enterprise Admin, you have selected the following users to help you with your pilot project: Alex Wilber, Joni Sherman, Lynne Robbins, Patti Fernandez, as well as the system admin, whose user account is the MOD Administrator.

Each user is a key member of your pilot project team. While their user accounts are already present in Microsoft 365, you need to configure their passwords so that they can more easily sign into Microsoft 365 when needed in the upcoming lab exercises. You also need to add a Microsoft 365 group that will be used in a later lab exercise.

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

   On the **Microsoft 365 admin center** tab, select the user icon for the **MOD Administrator** (the **MA** circle) in the upper right 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 your browser tabs except for your current 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 **Microsoft Office Home** tab, in the column of Microsoft 365 app icons that appear on the left side of the screen, scroll down and select the **Admin** icon; this opens 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**, in the left-hand navigation pane, select **Users**, and then under it, select **Active users**.

10. In the **Active Users** window, when you hover your mouse over a user's **Display name** (or you select the check mark field to the left of the **Display name**), a **key icon** appears to the right of the user's name. By selecting the key icon, you can reset a user's password. You need to reset Alex, Joni, Lynne, and Patti's passwords to **Pa55w.rd**.

    Select the key icon for **Alex Wilber**.

11. In the **Reset password** pane for Alex, select **Let me create the password**, enter **Pa55w.rd** in the **Password** field, select and copy this value so that you can paste it in for Joni and Lynne's accounts, and then unselect the **Require this user to change their password when they first sign in** check box.

12. Select **Reset** and then select **Close**.

13. Repeat steps 10-12 for **Joni Sherman**, **Lynne Robbins**, and **Patti Fernandez**. For these three accounts, paste in the **Pa55w.rd** password that you copied for Alex. You do not need to change the password for the **MOD Administrator** because you must continue using the default password provided by your lab hosting provider for this tenant admin account.

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

15. In the **Active groups** window, select **Add a group** that appears on the menu bar.

16. In the **Choose a group type** pane, select **Microsoft 365 (recommended)** and then select **Next**.

17. In the **Set up the basics** pane, enter **Sales Group** in the **Name** field. You must select the **Description** field to enable the **Next** button. Leave the **Description** field blank and select **Next**.

18. In the **Assign owners** pane, enter **Joni** in the **Owners** field. A list of users whose name starts with Joni will appear; select **Joni Sherman** and then select **Next**.

19. In the **Edit settings** pane, enter **salesgroup** in the **Group email address** field (Note: the domain should be the xxxxxZZZZZZ.onmicrosoft.com domain, which you should have verified in a prior task is the default domain for Adatum).

    Under the **Privacy** section, select the **Public – Anyone can see group content** option (even if this option is selected by default, select it again to enable the **Next** button), and leave the **Create a team for this group** check box selected. Select **Next**.

20. In the **Review and finish adding group** pane, review your selections. If anything needs to be corrected, select the corresponding **Edit** option. When everything is correct, select **Create group**.

21. Once the group is created, select the **Close** button on the **New group created** window.

22. This will return you to the **Groups** window. You may need to select the **Refresh** option on the menu bar for the **Sales Group** to appear in the list of groups. In fact, you may have to wait a few minutes for the Sales Group to appear, so you may need to select the **Refresh** option on the menu bar once or twice.

23. Once the **Sales Group** appears in the list of groups, select it.

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

25. In the **Members** tab, under the **Owners** section, Joni Sherman should appear as the only group owner. Under the **Members** section, select **View all and manage members**.

26. In the **View members** window for the Sales Group, select the **+Add members** button.

27. In the list of users that appears, select **Alex Wilber, Joni Sherman**, and **Lynne Robbins**, select the **Save** button, and then select the **Close** button to finish the add process.

    Note: You will not add Patti Fernandez to this group. Patti's key role in the pilot project is to test the Privileged Identity Management functionality in the next lab exercise.

28. The **Sales Group** window now displays the three members of the group. Select **Close**.

29. Close the **Sales Group** pane by selecting the **X** in the upper right-hand corner.

30. Leave the **Microsoft 365 admin center** tab open in your browser and proceed to the next task.

3.0.5 Task 5 - Enable IRM for SharePoint Online

In this task, you will turn on Information Rights Management (IRM) for SharePoint Online.

Note: While you will validate IRM for Exchange and SharePoint in Lab 4, you must enable IRM for SharePoint Online now because it can take up to 60 minutes or more for IRM to show up in SharePoint Online. By the time you get to the validation exercise in Lab 4, IRM should have finished its internal configuration and you won't have to wait for it to be present in SharePoint Online.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In the **Microsoft 365 admin center**, select **Show all** (if necessary) in the left-hand navigation pane to see all the navigation options. Under **Admin centers,** select **SharePoint**. This will open the SharePoint admin center.
3. In the **SharePoint admin center**, in the left-hand navigation pane, select **Settings**.
4. At the bottom of the **Settings** page is a sentence that says **Can't find the setting you're looking for? Go to the classic settings page.** In this sentence, select the hyperlinked text: **classic settings page**.
5. On the classic **Settings** page, scroll down to the **Information Rights Management (IRM)** section, select the **Use the IRM service specified in your configuration** option, and then select the **Refresh IRM Settings** button.
6. This will return you to the top of the **Settings** page. You must scroll to the bottom of the page to select the **OK** button. In doing so, when you get to the **Information Rights Management (IRM)** section, verify the **Use the IRM service specified in your configuration** option is selected and a **We successfully refreshed your settings** message appears below the **Refresh IRM Settings** button. Continue scrolling to the bottom of the page and select **OK**.
7. This will return you to the top of the **Settings** page. In your browser, close the current tab (the **xxxxxZZZZZZ-admin.sharepoint.com** tab).
8. Do **NOT** close the **SharePoint admin center** tab in your Edge browser. Leave your browser open for the next task.

3.0.6 Task 6 – Turn on Audit Logging to enable Alert Policies

In Lab 3, you will create Alert Policies using the Security and Compliance Center. However, before you can implement alerts, an admin must first turn on Audit Logging for the organization. Since it can take a couple of hours for audit logging to become fully enabled once you turn it on, you will turn it on in this lab so that it's fully enabled by the time you get to Lab 3.

Note: If you see an error message, "Fail to opt in, please refresh", Audit Logging is being enabled in the background and the message can safely be ignored.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.

   Select the **Microsoft 365 admin center** tab in your Edge browser.
2. In the **Microsoft 365 admin center**, select **Show all** (if necessary) in the left-hand navigation pane to see all the navigation options. Under **Admin centers,** select **Security**. This will open the Office 365 Security and Compliance center.
3. In the **Office 365 Security & Compliance center**, in the left-hand navigation pane, select **Search**, and then under it, select **Audit log search**.
4. In the **Audit log search** window, a warning message is displayed at the top of the page. Select the **Turn on auditing** button that appears on the right-side of this message, and then in the **Security & Compliance** dialog box that appears, select **Yes** to confirm that your organization settings need to be updated.

   Note: It may take several minutes for the setting to be updated, at which time the **Security & Compliance** dialog box will disappear.
5. Leave the Client 1 VM and the Security and Compliance Center open and proceed to the next lab.

3.0.7 Task 7 – Prepare Users for Content Searches

In Module 8, you will perform a Content Search lab that requires that Joni Sherman and Holly Dickson be members of the eDiscovery Manager role. In this exercise, you will add Joni and Holly to this role. The reason you are doing this now is that it can sometimes take up to an hour or more for newly assigned permissions to successfully propagate. If you waited and assigned Holly and Joni to this role group at the time you performed the Content Search lab in Module 8, you would receive error messages involving parameter fields because their permissions would not have finished propagating. By adding them to this role group now, enough time will elapse for the propagation to complete by the time you get to the Module 8 lab.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, you should still have the **Office 365 Security and Compliance Center** open in a tab from the prior task. If you closed that tab, then in the **Microsoft 365 admin center**, under the **Admin centers** group, select **Security**.
3. In the **Office 365 Security and Compliance Center**, in the left-hand navigation pane, select **Permissions.**
4. In the **Home > Permissions** page, select the **eDiscovery Manager** check box.
5. In the **eDiscovery Manager** pane that appears, scroll down to the **eDiscovery Manager** section and select **Edit**.
6. The **Editing Choose eDiscovery Manager** wizard opens. The list of users who are assigned this role should be empty. Select **Choose eDiscovery Manager**.
7. In the **Choose eDiscovery Manager window**, select **(+) Add**.
8. In the list of users that's displayed, select **Joni Sherman** and **Holly Dickson**, select **Add**, and then select **Done**.
9. In the **Editing Choose eDiscovery Manager** window, select **Save**.
10. In the **eDiscovery Manager** window, select **Close**.
11. Leave your browser open and do not close any of the tabs.

4 End of Lab 1

5 Module 1 - Lab 1 - Exercise 2 - PIM Resource Workflows

As part of her Microsoft 365 pilot project, Holly Dickson, Adatum's Enterprise Administrator, wants to implement Privileged Identity Management within Azure Active Directory. One of Adatum's pain points in their existing system is they have far too many users who have been assigned administrator roles. This has caused concern among management, who sees this as a threat to Adatum's data security. They feel that too many people were assigned admin roles that shouldn't have been, and as such, they have access to secure information and resources that could potentially compromise the organization.

Because there is a need to reduce the number of users with permanent administrator roles and yet still provide admin privileges to selected users when business justification warrants it, Holly has been tasked with implementing Azure Active Directory's Privileged Identity Management service. By implementing PIM, Adatum can reduce the number of users with admin roles and yet still be able to assign users with admin rights on an as-needed basis whenever necessary.

In this lab, you will perform the basic steps involved in implementing PIM for a given admin role:

- Configure the role to require approval and assign an approver
- Assign an eligible user to the role
- Submit a request from the eligible user to be assigned the role
- Approve the request for the role

In this exercise, you will perform these tasks for the Global administrator role. Holly will take on the role of the approver, and Patti Fernandez will be the user requesting access to the role.

IMPORTANT: In Task 3, Patti Fernandez will submit a request to be assigned the Global administrator role. The activation request process is set up to require Multi-Factor Authentication (MFA). If you do not have a

phone to complete this process, notify your instructor. You can still complete Tasks 1 and 2, and you may be able to partner up with another student to watch them complete the remaining tasks.

5.0.1 Task 1 - Configure the Global Administrator role to require approval

Since the Microsoft 365 Global Administrator role provides a user with basically unlimited access to all Microsoft 365 resources, the number of users assigned to this role should obviously be kept to a minimum for security purposes.

Holly Dickson, Adatum's Enterprise Administrator, wants to limit access to this role using Privileged Identity Management. To do so, she must first configure the role to require approval before it can be assigned as an eligible role for a user, and then she wants to assign herself as the approver whenever an eligible user requests activating the role.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as Holly Dickson from the previous lab exercise.
2. In your browser, select the **Microsoft 365 admin center** tab. In the left-hand navigation pane under the **Admin centers** section, select **Azure Active Directory**
3. In the **Azure Active Directory admin center**, in the left-hand navigation pane, select **All services**.
4. In the **All services** window, the services are separated into three sections - General, Identity, and Services. Under the **Identity** section, select **Azure AD Privileged Identity Management**.
5. In the **Privileged Identity Management | Quick start** window, note how the window is divided into three parts - the navigation pane on the left, the middle pane (which provides navigation options for this page), and the detail pane on the right.

   In the middle pane under the **Manage** section, select **Azure AD roles**.
6. In the **Adatum Corporation | Quick start** window, in the middle pane under the **Manage** section, select **Settings**.
7. In the **Adatum Corporation | Settings** window, select the **Global Administrator** role.
8. In the **Role setting details - Global Administrator** window, select **Edit** on the menu bar at the top of the page.
9. In the **Edit role setting - Global Administrator** window, select the **Require Approval to activate** check box.
10. In the **Select approver(s)** section, no specific approver has been selected. Holly wants to assign herself as the approver for this role, so select this section. In the **Select a member** pane that opens on the right, scroll down through the list of users and select **Holly Dickson**, and then select the **Select** button.
11. In the **Edit role setting - Global Administrator** window, select **Update**.
12. Leave all browser tabs open for the next task.

5.0.2 Task 2 - Assign an eligible user to the Global Admin role

For Adatum's PIM pilot project, Holly has selected Patti Fernandez as the sole user who will be eligible to be assigned the Global admin role. In this task, Holly will enable Patti to be eligible for the Global admin role.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as Holly Dickson.
2. In your **Edge** browser, you should still have the **Azure Active Directory admin center** open in a tab that's displaying the **Adatum Corporation | Settings** window. In the navigation thread at the top of the page (**All services > Privileged Identity Management > Adatum Corporation**), select **Privileged Identity Management**.
3. In the **Privileged Identity Management | Quick start** window, in the middle pane under **Manage**, select **Azure AD roles**.
4. In the **Adatum Corporation | Quick start** window, the detail pane on the right displays the **Privileged Identity Management** window. This displays three groups - Assign, Activate, and Approve. Under the **Assign** group, select **Assign Eligibility**.

5. In the **Adatum Corporation | Roles** window, scroll down through the list of roles and select **Global Administrator**.
6. In the **Global Administrator | Assignments** window, select **+Add assignments** on the menu bar.
7. In the **Add assignments** window, the **Membership** tab is displayed by default. Scroll down on the page, and under **Select member(s)**, select **No member selected**.
8. In the **Select a member** pane that appears on the right, scroll down through the list of users and select **Patti Fernandez**, and then select the **Select** button.
9. In the **Add assignments** window, select **Next** (this does the same thing as selecting the **Setting** tab).
10. In the **Add assignments** window, under the **Settings** tab, verify the **Assignment type** option is set to **Eligible**, and then select **Assign**.
11. In the **Global Administrator | Assignments** window, note that Patti Fernandez is now an eligible user who can be assigned the Global Administrator role.

    Note: It can take 30 minutes for the **Pending Request** to be implemented. Wait at least 10 minutes, then refresh the **Global Administrator | Assignments** window until you see Patti listed under the **Eligible assignments** tab.
12. Leave all browser tabs open for the next task.

5.0.3 Task 3 - Submit a request for the Global Admin role

Now that Patti Fernandez has been made an eligible user for the Global administrator role, Holly wants to test out the PIM process in her pilot project. In this task, Patti will submit a request to be assigned Global administrator role privileges. In the next task, Holly will review her request and approve it.

Note: The activation request process is set up to require Multi-Factor Authentication (MFA). If you do not have a phone to complete this process, notify your instructor. You may be able to partner up with another student to watch them complete the remaining two tasks.

1. In LON-CL1, right-click on the **Edge** icon on the taskbar and in the menu that appears, select **New InPrivate window**.
2. In your InPrivate browser session, enter the following URL in the address bar: **https://portal.azure.com**
3. In the **Sign in** window, enter **PattiF@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**. In the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes**.
4. In the **Welcome to Microsoft Azure** dialog box that appears, select **Maybe later** to skip the tour.
5. In the **Microsoft Azure** portal, scroll down to the **Azure services** section, and then on the right side of the section, select **More services**.
6. In the **All services** window, enter **priv** in the **Search** box at the top of the page. In the list of search results, select **Azure AD Privileged Identity Management**.
7. In the **Privileged Identity Management | Quick start** window, in the **Tasks** section in the left-hand navigation pane, select **My Roles**.
8. In the **My roles | Azure AD roles** window, the **Eligible assignments** tab is displayed by default. Since Holly assigned Patti as an eligible user for the Global Administrator role, this role appears in the list. Under the **Action** column for the Global Administrator role, select **Activate**.
9. In the **Activate - Global Administrator** pane, a warning message is displayed at the top of the pane indicating additional verification is required. Select this message, which is hyperlinked.
10. In the **More information required** window that appears, select **Next**.
11. In the **Enter password** window, enter **Pa55w.rd** in the Password field and then select **Sign in**.
12. On the **Microsoft Authenticator** page, you can download this mobile app or use a different method for MFA verification. For the purposes of this lab, we recommend you use your mobile phone so that you do not have to take time installing the Microsoft Authenticator app that you may not use again after this training class. Select the **I want to set up a different method** option at the bottom of the page.

13. On the **Choose a different method** dialog box that appears, select the drop-down arrow in the **Which method would you like to use?** field, select **Phone**, and then select **Confirm**.
14. In the **Phone** window that appears, under **What phone number would you like to use?** field, select your country or region, and then in the field next to it, enter your phone number (in the format **nnn-nnn-nnnn**). Verify the **Text me a code** option is selected and then select **Next**.
15. Retrieve the verification code from the text message that is sent to your phone.
16. In the **Phone** window, enter the 6 digit verification code in the **Enter code** field and then select **Next**.
17. Once verification is complete and you receive a message indicating your phone was registered successfully, select **Next**.
18. On the **Success!** page, select **Done**.
19. If you receive a dialog box indicating your sign in has timed out, you will have to enter Patti's password of **Pa55w.rd** and then you will be sent another verification code to your phone. On the **Enter code** window, enter this new code and then select **Verify**.
20. If you take too long to complete this process, the **Enter password** window will appear with a message indicating you took too long to complete the sign in process, so you will be timed-out. If this occurs, you must sign in again with Holly's password of **Pa55w.rd**. Another verification code will be texted to your phone, so enter it in the **Enter code** screen that appears and select **Verify**.
21. In the **Activate - Global Administrator** pane that appears, enter **Testing PIM** in the **Reason** field, and then select the **Activate** button at the bottom of the pane.
22. On the **My roles | Azure AD roles** window, the **Eligible assignments** tab is displayed on the menu bar. Select the **Active assignments** tab that appears next to it. Note that no roles appear.

    Note: If you recall, back in Task 1 Holly set up the Global Administrator role so that activation to a user account will require approval. What Patti just did was request that the Global Admin role be activated for her user account. This will send a request to Holly, who can then either approve or deny Patti's request for role activation. Holly will review this request in the next task.
23. Leave the InPrivate browser session open. You will return to it in the next task once Holly approves Patti's request.

5.0.4 Task 4 - Approve the request for the Global Admin role

Back in Task 1, Holly set herself up as the approver for the Global Administrator role. Since Patti has submitted a request to be assigned this role, Holly must review the request and determine whether to accept or deny it.

1. In LON-CL1, you currently have the InPrivate Browser session open. Select the Edge icon on your taskbar to see windows for the two Edge sessions that you have open - the window on the left is the original Edge browser session in which you are signed into **Microsoft 365** as **Holly Dickson**, and the window on the right is the InPrivate Browser session in which you are signed into **Azure AD** as **Patti Fernandez**. Select the window on the left to go back to the original Edge browser session in which you are signed in as **Holly Dickson**.
2. In your browser, select the **Global Administrator | Assignments** tab. This should display the **Global Administrator | Assignments** window in the **Azure Active Directory admin center**.

    In the navigation thread at the top of the page (**All services > Privileged Identity Management > Adatum Corporation**, select **Privileged Identity Management**.
3. In the **Privileged Identity Management | Quick start** window, in the middle pane under **Tasks**, select **Approve requests**.
4. In the **Approve requests | Azure AD roles** window, in the **Requests for role activations** section, select the check box to the left of the Global Administrator request from Patti Fernandez, and then select the **Approve** button.
5. In the **Approve Request** pane that appears, enter **PIM testing** in the **Justification** field and then select **Confirm**.
6. Switch back to the InPrivate browser session where Patti is signed in. In the **My roles | Azure AD roles** window that should still be displayed, the **Active assignments** tab is currently selected from the

prior task, prior to approving Patti's request. Select **Refresh** on the menu bar. Note how the Global Administrator role is now activated for Patti.

7. Close the InPrivate browser session.
8. In your Edge browser session, close all the tabs except for the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab. Leave these two tabs open for the next lab.

6 End of Lab 1

7 Module 2 - Lab 2 - Exercise 1 - Implement a Safe Attachments policy

You now have a Global admin account set up for Holly Dickson, and you're signed into Microsoft 365 as Holly. In this first phase of your pilot project for Adatum, you want to create a Safe Attachments policy and turn on Microsoft Defender for Office 365, which provides advanced threat protection for SharePoint, OneDrive, and Microsoft Teams.

Note: You will not be able to validate the Safe Attachments policy. To do so would require that you attach a virus or malware-infected file to an email, which is something that Microsoft does not recommend.

7.0.1 Task 1 – Create a Safe Attachment policy and turn on ATP for SharePoint, OneDrive, and Microsoft Teams

In this task, you will turn on Windows Defender for Office 365, which provides advanced threat protection (ATP) for SharePoint, OneDrive, and Microsoft Teams. You will also create a Safe Attachments policy that will test email attachments for malware that are sent to recipients within the xxxxxZZZZZZ.onmicrosoft.com domain. You will configure the policy so that if an attachment is blocked, it will be removed from the email that is sent to the recipient, and a copy of the email will be redirected to Joni Sherman for additional review.

1. You should still be logged into your Client 1 VM as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, select the **Microsoft 365 admin center** tab. In the left-hand navigation pane, under **Admin centers**, select **Security**. This will open a new tab in your browser for the **Office 365 Security & Compliance center**.
3. In the **Office 365 Security & Compliance center**, in the left-hand navigation pane select **Threat Management** and then select **Policy**.
4. In the **Policy** window, double-click the **Safe Attachments** tile.
5. In the **Safe attachments** window, on the menu bar, select **Global settings**.
6. In the **Global settings** pane that appears, set the following options and then select **Save**:
   - **Turn on Defender for SharePoint, OneDrive and Microsoft Teams** - set the toggle switch to **On** (this enables Windows Defender for Office 365, formerly known as Advanced Threat Protection, or ATP)
   - **Turn on Safe Documents for Office clients** - set the toggle switch to **On**
7. On the **Safe attachments** window, select **+Create** on the menu bar to initiate the **New Safe Attachment Policy** wizard.
8. On the **Name your policy** page, enter **AttachmentPolicy1** in the **Name** field and then select **Next**.
9. On the **Settings** page, select the **Dynamic Delivery** option. This option will still send the email but will hold the attachment until it has been scanned and marked acceptable.
10. Scroll to the bottom of the **Settings** page and select the **Enable redirect** check box.
11. In the **Send the attachment to the following email address** field, enter **JoniS@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), and then select **Next**.
12. If a **Security & Compliance** dialog box appears with a WARNING message about the Enable Redirect option, select **OK**.

13. On the **Applied to** page, select the **+Add a condition** button. In the drop-down menu that appears, under the **Applied if...** section, select **The recipient domain is...**
14. In **The recipient domain is** section, select the **Choose** link to choose a domain.
15. In **The recipient domain is** window, select the **+Add** button. In the list of domains that appear, select the check box for the **xxxxxZZZZZZ.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), select **Add**, and then select **Done**.
16. On the **Applied to** page, select **Next**.
17. On the **Review your settings** page, review the options that you selected. If any need to be corrected, select the appropriate **Edit** option and make the correction. If they all appear correct, select **Finish**.
18. If a **Security & Compliance** dialog box appears with a message about updating your organization settings, select **Yes**.

    It may take a minute or so to update the organization settings. Once the settings are updated, the **AttachmentPolicy1** policy that you created will appear in the Safe attachments list.
19. Leave the Client 1 VM and the Security & Compliance Center tab open for the next lab.

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

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

8 Proceed to Lab 2 - Exercise 2

9 Module 2 - Lab 2 - Exercise 2 - Implement a Safe Links Policy

Now that you have created a Safe Attachments policy for Adatum, you want to create a Safe Links policy and then validate the policy to ensure that it works properly.

IMPORTANT: This lab exercise consists of two tasks. The first task creates a Safe Links policy, and then the second task validates the policy. The problem with this lab is that when you create a safe links policy, it takes at least 30 minutes for the policy to propagate through the system. **This means that you can perform the first task, but then you must wait at least 30 minutes before you can perform the final task.** You should continue with the training class and your instructor will provide guidance on when you can perform Task 2 depending on the next break that occurs in the class schedule.

9.0.1 Task 1 – Create a Safe Links Policy

In this task, you will create a Safe Links policy that applies to all users in your tenant. You will then add the **http://tailspintoys.com** URL to the company-wide list of blocked URLs that you will define in the Safe Links global settings. The blocked URLs and other options defined in the Safe Links global settings are only applied to users who are included in active Safe Links policies. There is no built-in or default Safe Links policy, so you must create at least one Safe Links policy for these global settings to be active.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. After finishing the previous task, you should still be in the **Microsoft 365 Security and Compliance center**. If not, in your browser, enter **https://protection.office.com.**
3. In the **Security & Compliance center**, in the left-hand navigation pane, the **Threat Management** group should still be expanded from the prior task; if not, expand it now. Under this group, select **Policy**.
4. In the **Policy** window, double-click the **Safe Links** tile.

5. On the **Safe links** page, select **+Create** on the menu bar. This initiates the **Create Safe Links Policy** wizard.
6. On the **Name your policy** page, enter **LinkPolicy1** in the **Name** field and then select **Next**.
7. On the **Settings** page, enter the following settings and then select **Next**:
   - Select the action for unknown or potentially malicious URLs in messages - **On**
   - Select the action for unknown or potentially malicious URLs within Microsoft Teams - **Off**
   - Apply real-time URL scanning for suspicious links and links that point to files - select this check box
   - Wait for URL scanning to complete before delivering the message - select this check box
   - Apply safe links to email messages sent within the organization - select this check box
   - Do not track user clicks - select this check box
   - Do not allow users to click through to original URL - select this check box
8. On the **Applied to** page, select **+Add a condition**. In the drop-down menu that appears, under the **Applied if...** section, select **The recipient domain is**
9. In **The recipient domain is** section, select the **Choose** link to choose a domain.
10. In **The recipient domain is** window, select the **+Add** button. In the list of domains that appear, select the check box for the **xxxxxZZZZZZ.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), select **Add**, and then select **Done**.
11. On the **Applied to** page, select **Next**.
12. On the **Review your settings** page, review the options that you selected. If any need to be corrected, select the appropriate **Edit** option and make the correction. If they all appear correct, select **Finish**. Once the **LinkPolicy1** policy is created, it will appear in the Safe links list.
13. On the **Safe links** page, select **Global settings** on the menu bar.
14. In the **Safe Links policy for organization** pane that appears, enter **http://tailspintoys.com** in the **Block the following URLs** field, do NOT change the default settings for any of the other options, and then select **Save**.
15. Leave the Office 365 Security & Compliance tab open for the next task.

STOP!! As mentioned at the start of this lab exercise, now that you have created a Safe Links policy, you must wait at least 30 minutes for the policy to propagate through the system before you can perform the next task in this exercise.

Do NOT proceed to the next task! You can continue with the training course and perform the next task when your instructor feels it's appropriate given the class training schedule.

9.0.2 Task 2 – Validate the Safe Links Policy

In this task, you will test the Safe Links Policy that you just created that blocks links to the http://tailspintoys.com URL.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, select the **Microsoft Office Home** tab and then in the column of app icons on the left side of the screen, select the **Outlook** icon.
3. **Outlook** will open in a new tab in your browser, and Holly's **Inbox** will be displayed.
4. Select the **New Message** button in the upper left part of the screen.
5. In the email form that appears in the right-hand pane, enter the following information:
   - To: You will be sending an email to the MOD Administrator, so enter **mod** in the **To** field and then select the **MOD Administrator** email address from the user list.
   - Add a subject: **Free stuff for Adatum users**
   - body of the message: **Please click on me for free toys from TailSpin Toys.**
6. Select the text that you added in the body of the message.

7. Below the body of the message is a long row of formatting icons. Select the **Insert link** icon, which depicts two overlapping circles.
8. In the **Insert link** window, the text that you highlighted in the body of the message should be displayed in the **Display as** field. In the **Web address (URL)** field, enter the following URL: **http://tailspintoys.com/aboutus/freetoys**.
9. Select **OK**.
10. In the body of the email, the message should still be selected. Click anywhere in the body of the message to remove the highlighting. The color of the text should now be blue, and it should be underlined, indicating that this message is hyperlinked to a URL.
11. Select either **Send** button (top or bottom of the form).
12. You now want to go the MOD Administrator's Inbox in Outlook and validate whether the Safe Links policy you created in the prior task worked on the email that you just sent from Holly to the MOD Administrator.

    To do this, you must first switch the Client 2 VM (**LON-CL2**).
13. Log into the LON-CL2 VM as the **Admin** account by entering **Pa55w.rd** in the **Password** field.
14. Select the **Microsoft Edge** icon in the taskbar, maximize the window and then enter the following URL in the address bar: **https://outlook.office365.com**
15. In the **Sign-in** window, enter **admin@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 the tenant password provided by your lab hosting provider and select **Sign in**.
17. Close the **Let Microsoft Edge save and fill your password for this site next time?** banner by selecting **Never**.
18. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
19. In the **Welcome** windows, select the X in the upper right corner to close the window.
20. In the MOD Administrator's **Inbox**, open the email that was sent by Holly.
21. Select the hyperlink in the body of the message to open it.
22. If a window opens indicating the new browser recommended by Microsoft is here, select **No thanks**.
23. A new tab should open in your **Edge** browser that takes you to the URL you just saw in the prior step. This site should display the following warning message: **This website has been blocked per your organization's URL policy.** This not only indicates that opening this website might not be safe, but it also verifies that the Safe Links policy you just created is working properly.
24. In LON-CL2, leave the Edge browser and all its tabs open for the next lab.

10 End of Lab 2

11 Module 3 - Lab 3 - Exercise 1 - Conduct a Spear Phishing attack using the Attack Simulator

Holly Dickson is concerned that some users at Adatum may require education about phishing attacks. As part of her pilot project, Holly has decided to use the Microsoft 365 Attack Simulator to determine her users' susceptibility to phishing attacks.

11.0.1 Task 1: Enable Multi-factor Authentication for the Global Admin

To use Microsoft's Attack Simulator to simulate a phishing attack, you must first enable Multi-Factor Authentication (MFA) for either your entire organization or for just the Global admin who will run the simulator. For her pilot project, Holly does not want to set up MFA for all the Adatum users at this point in time; therefore, she will enable MFA for her user account only, and then after she finishes running the Attack Simulator, she will turn MFA back off.

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

1. Switch to the **LON-CL1** VM, where you should still be logged in as the **Admin** account. If necessary, log in as the **Admin** with a password of **Pa55w.rd**.
2. In your **Edge** browser, you should still be logged into Microsoft 365 as Holly Dickson. Select the tab containing the **Microsoft 365 Security** center, which should still be open from the Safe Links lab that you just completed.
3. In the **Microsoft 365 Security** center, in the left-hand navigation pane under **Email and collaboration**, select **Attack simulation training**.
4. On the **Attack Simulation taining** page, scroll down to see the four types of attacks that you can simulate. Also note the warning message that indicates you must enable multi-factor authentication (MFA) to schedule or terminate attacks. This is required because the system wants to confirm your credentials before you conduct a simulated attack. In the upcoming steps, you will enable MFA for Holly and then perform a phishing attack.
5. To enable MFA for Holly Dickson's user account, select the **Microsoft 365 admin center** tab in your browser, and then in the left hand-navigation pane, select **Users** and then select **Active users**.
6. In the **Active users** window, on the menu bar at the top of the user list, select **Multi-factor authentication**. If it does not appear, select the **ellipsis (More actions)** icon. In the drop-down menu that appears, select **Multi-factor authentication**.
7. In the **multi-factor authentication** window, the **users** tab is displayed by default. Note the MFA status for all existing user accounts, which is **Disabled**. Select the check box for **Holly Dickson**, and in Holly's properties pane that appears on the right, select **Enable**.
8. On the **About enabling multi-factor auth** dialog box, select **enable multi-factor auth**.
9. When the **Updates successful** dialog box appears, select **close**. In the **multi-factor authentication** window, verify Holly's MFA Status has changed to **Enabled**.
10. You must now sign out of Microsoft 365 as Holly, close your browser session (to clear cache), open a new session, and then log back in as Holly using MFA. The first time you sign back in after having MFA enabled for your user account, you will be asked for the authentication information needed for MFA, such as your phone number and authentication options. You will then be texted a verification code to validate the authentication process works. You will perform these steps in the remaining portion of this task.

    You must begin by signing out of Microsoft 365 as Holly, so select the **HD** user icon in the upper right corner of the browser and in the **Holly Dickson** window that appears, select **Sign out**.
11. Once you are signed out, close the browser session and all the browser tabs.
12. Select the **Edge** icon on your taskbar to open a new browser session, and then navigate directly to the **Microsoft 365 Security** center by entering the following URL in the address bar: **https://Security.Microsoft.com**
13. In the **Sign in** window, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**. In the **Enter password** window, enter **Pa55w.rd** and select **Sign in**.
14. Because MFA is enabled for Holly, a **More information required** window appears. Select **Next**.
15. On the **Microsoft Authenticator** page, you can download this mobile app or use a different method for MFA verification. For the purposes of this lab, we recommend you use your mobile phone so that you do not have to take time installing the Microsoft Authenticator app that you may not use again after this training class. Select the **I want to set up a different method** option at the bottom of the page.
16. On the **Choose a different method** dialog box that appears, select the drop-down arrow in the **Which method would you like to use?** field, select **Phone**, and then select **Confirm**.
17. In the **Phone** window that appears, under **What phone number would you like to use?** field, select your country or region, and then in the field next to it, enter your phone number (in the format **nnn-nnn-nnnn**). Verify the **Text me a code** option is selected and then select **Next**.

18. Retrieve the verification code from the text message that is sent to your phone.
19. In the **Phone** window, enter the 6 digit verification code in the **Enter code** field and then select **Next**.
20. This takes you back to the **Microsoft Authenticator**, Select the **I want to set up a different method** option at the bottom of the page.
21. On the **Choose a different method** dialog box that appears, select the drop-down arrow in the **Which method would you like to use?** field, select **Email**, and then select **Confirm**.
22. Enter your personal email address and select **Enter**.
23. Open your personal email address and the email from Adatum corporation. Note the verification code.
24. Enter the verification code from the Adatum email to your personal email address then select **Next**.
25. On the **Success!** page, select **Done**.
26. If you receive a dialog box indicating your sign in has timed out, you will have to enter Patti's password of **Pa55w.rd** and then you will be sent another verification code to your phone. On the **Enter code** window, enter this new code and then select **Verify**.
27. If you take too long to complete this process, the **Enter password** window will appear with a message indicating you took too long to complete the sign in process, so you will be timed-out. If this occurs, you must sign in again with Holly's password of **Pa55w.rd**. Another verification code will be texted to your phone, so enter it in the **Enter code** screen that appears and select **Verify**.
28. The **Microsoft 365 Security** center should now be displayed in your browser. You will resume from here in the next task when you launch a spear phishing attack using the Attack Simulator. Leave this tab open in your browser.
29. You have now configured MFA, you have signed into the **Micosoft 365 Security** center using MFA, and you are ready to run the Attack Simulator. Leave everything as is in your VM and proceed to the next task.

11.0.2 Task 2: Configure and launch a Spear Phishing attack

Now that Holly has turned on MFA, she is ready to run the Attack Simulator and launch a simulated spear phishing attack. This will provide visibility into how well Adatum is prepared to handle such a security attack.

1. You should still be on **LON-CL1**, and you should still be logged in as the **Admin** account. If necessary, log in as the **Admin** with a password of **Pa55w.rd**.
2. You should still have the **Microsoft 365 Security** center open in in your **Edge** browser from the prior task. If not, enter **https://Security.Microsoft.com** in the address bar, and then when you receive the dialog box asking for a second form of authentication, proceed through the verification process.
3. In the **Microsoft 365 Security** center, under **Email & collaboration** in the left-hand navigation pane and then select **Attack simulation training**.
4. On the **Attack Simulation training** page, you reviewed the four types of simulated attacks that are available in the prior task. For this simulation, Holly has decided to conduct an account breach in which she will use a URL to try and obtain usernames and passwords. This is referred to in the Attack Simulator as a **Credentials Harvest** attack.

   You can launch this attack either from **Simulations** tab or selecting the **Launch a simulation** link on the **Overview** page.. Since the **Overview** tab has additional information and is the default page when selecting the **Attack simulation training** service, it is recommended that you launch it from there so that you can learn about the specifics of this type of attack.

   To the right of the **Credentials Harvest** section, select **Launch a simulation**.
5. On the **Launch a simulation** page, review the specific information related to the **Credentials Harvest** attack type.
6. In the **Select Technique** section for the **Credentials Harvest** attack type, select **Next**.
7. In the **Simulation** wizard, the steps involved in the simulation are displayed in the left-hand pane. While you can manually create a phishing campaign, it is recommended that you take advantage of the available templates that will prefill most of the information for you. The key to a successful phishing attack is to create a very intriguing, real-world looking email, and the templates provide very creative solutions.

On the **Name Simulation** page, provide the following information the **** button.

- Simulation Name : **PhishingTest1**
- Description : **This simulation is to provide insight on targeted email threats agianst users inside the company.**

8. Select **Next**.
9. on the **Select Payload** screen. Select **2 failed Messages** from the **applied filters** menu. when you select this option a window should open on the left hand side to give you a view of the email that will be sent to the users, then select **Next**.
10. From the **Target Users** screen. Select **include all users in my organization**. this will give you a view of every user inside your orgainzation. Select **Next**.
11. On the **Assign Training** screen. Leave **Preferences** as reccommend and leave **Assign training for me** as the selection option. Change **Due Date** to **7 days after Simulation ends** then select **Next**.
12. On the **Launch Details**screen. Select **Launch this simulation as soon as I'm done.**Then select **Next**.
13. On the **Review Simulation** screen. Review the entered information and select **submit**. A few moments will pass and you will recieve a confirmations stating **Simulation has been scheduled for launch**. Select **Done**

11.0.3 Task 3: Review the attack simulation results

In this task, you will verify whether your orgainization has received the email that you configured in the Attack simulation training, and then you will review the report associated with the Spear Phishing attack that you simulated.

1. Switch to the **LON-CL2** VM and log in as the **Admin** with a password of **Pa55w.rd**.
2. In the Edge browser, in the **Outlook** tab in which you are signed in as the MOD Administrator, select the **MA** initials in the upper right hand corner of the screen. In the **MOD Administrator** window that appears, select **Sign out**.
3. Close all browser tabs except for the **Sign out** tab. In the **Sign out** tab, enter the following URL in the address bar to navigate directly to Outlook on the web: **https://outlook.office365.com**.
4. In the **Pick an account** window, select **Use another account**.
5. In the **Sign in** window, enter **LynnR@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix ID provided by your lab hosting provider), and then in the **Enter password** window, enter **Pa55w.rd** and select **Sign in**.
6. Close the **Welcome** window.
7. In Lynne's Outlook Inbox, you should see the spear phishing email that was sent by the Attack Simulator. Select the email to open it and review the details in the body of the message.

   NOTE! It can take up to 15 minutes for the email to arrive. Wait for the email before proceeding.
8. Select the link that is included in the email. Even though you know this is a spear phishing attack, this will enable you to see the effect of doing so in the Attack Simulator report that tracks the results of the spear phishing campaign.
9. In the **Sign in** dialog box that appears, enter **LynnR@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix ID provided by your lab hosting provider), and then in the **Enter password** window, and select **Sign in**.
10. This displays a web page that explains how you have redirected to it as part of a Phishing awareness test being run by your organization. Read through the contents of this page.
11. Switch back to LON-CL1.
12. In your browser session where you are logged in as Holly Dickson, if you are still on the **Attack details** page, then scroll down to the **Attack History** section under **Credential Harvest** section and select the **Refresh** button. It should display details on your phishing attack. Select the right arrow to view the report on the phishing attack.

Note: If you were instead back on the **Attack simulator** page, then in the **Credential Harvest** section, below the **Attack Completed** message, select **View Report**.

13. On the **Report** page, review the report for the phishing campaign that you completed. Note the date and time of the report. If you had run a previous simulation, it sometimes take 60 minutes to update this report information with the details from the current simulation that you just ran. If this occurs, refresh the page after a few minutes. Review the information on the page and note the results after having selected the spear phishing URL in the email that was sent to Lynne Robbins earlier in this task.
14. Leave your browser open in LON-CL1 and do not close any of the tabs.

12 Proceed to Lab 3 - Exercise 2

13 Module 3 - Lab 3 - Exercise 2 - Conduct Password attacks using the Attack Simulator

Holly Dickson is concerned that some users at Adatum may require education about secure password strategies. In this lab she will use the Microsoft 365 Attack Simulator to determine her users' susceptibility to password attacks.

Note: At the end of this exercise, you will disable MFA for Holly's account. This will save you from having to enter the second form of authentication when signing in as Holly in any of the remaining labs in this course.

13.0.1 Task 1: Configure and launch a Brute Force attack

Password cracking techniques are used to guess a user's password by trying many variations with a computer. Once an attacker has the user name and password for a user, the attacker will generally be able to sign in to Microsoft 365 and gain access to additional information, such as other user accounts and sensitive information. Brute-force attacks work by calculating every possible combination that could make up a password and testing to see if it is the correct password.

Two types of brute-force password attacks exist: a dictionary attack using a well-known list of passwords, and an exhaustive attack, where combinations are tried sequentially. The Attack Simulator uses a dictionary list attack, allowing modifications of frequency between attacks and the number of attempts. If a password is discovered, the password itself is not shown; only an indication that a password was discovered will be shown.

For this lab, you will not include a file of passwords; you will instead enter a short list of passwords. For her pilot project, Holly is once again going to use Lynne Robbins as her test case.

1. You should still be in LON-CL1 and signed in as the **Admin** with a password of **Pa55w.rd**; if not, then sign in now.
2. After the previous lab exercise, you should still be in the **Office 365 Security and Compliance** center, and you should still be logged in as Holly Dickson; if not, then do so now.
3. After the previous lab exercise, you should also be in the **Attack Simulator**; if not, then in the left-hand navigation pane, under **Threat Management**, select **Attack simulator**. In the list of 4 attacks, scroll down to the **Brute Force Password (Dictionary Attack)** section and select the **Launch Attack** button.
4. In the **Provide a name for the password attack** page, enter **Brute Force Test** in the **Name** field and select **Next**.
5. In the **Select user accounts which to attempt the password attack** page, select the **Address Book** button, enter **Lynne** in the **Search** field, select **Lynne Robbins** from the resulting list of users, and then select **Next**.
6. In the **Choose attack settings** page, enter the following list of passwords. You MUST hit Enter after entering each password:
   - P@ssw0rd
   - Pa$$w0rd
   - PA$$WORD
   - P@55w0rd
   - Pa55w.rd

Note: You will enter Lynne's actual password on purpose to check the results when a password match occurs. Once you have added all the passwords, select **Next**.

Note: Ordinarily you would have a file that contains a list of commonly used passwords for your organization. You would upload that file using the **Upload** button.

7. In the **Confirmation** page, select **Finish** to run the simulation.
8. Once the attack is complete, you will be returned to the **Attack simulator** page.
9. Leave your browser and the Security and Compliance Center open for the next task.

13.0.2 Task 2: Review the Brute Force results

You will now review the results of the Brute Force Password attack.

1. In your browser session where you are logged in as Holly Dickson, you should still be on the **Attack simulator** page. In the **Brute Force Password Dictionary Attack)** section, it will display **Attack Completed** once the attack is done. Select the **Refresh** icon on the address bar to refresh the results. This may take several minutes to complete, so you may need to refresh your screen several times. Once the attack is complete, select **View Report**.
2. On the **Attack details** page, view the report for the **Brute force test** that you completed. Review the information on the page and note the results after having entered Lynne's actual password among the list of passwords that were entered for the simulation.
3. In the **Attack details** page, select **Attack simulator** in the navigation thread at the top of the page (**Home > Attack simulator > Report**).
4. Leave your browser open in LON-CL1 and do not close any of the tabs.

13.0.3 Task 3: Configure and launch a Password Spray attack

A password spray attack against an organization is typically done by running a list of commonly used passwords against a list of valid Microsoft 365 user accounts. Typically, the attacker crafts one password to try against all the known user accounts. If the attack is not successful, the attacker will try again using another carefully crafted password, usually with a waiting period between attempts to avoid policy-based account lockout triggers. For her pilot project, Holly is once again going to use Lynne Robbins as her test case.

1. You should still be in LON-CL1 and signed in as the **Admin** with a password of **Pa55w.rd**; if not, then sign in now.
2. In your browser session where you are logged in as Holly Dickson, you should be on the **Attack simulator** page.
3. In the list of 4 attacks, scroll down to the **Password Spray Attack** section and select the **Launch Attack** button.
4. In the **Provide a name for the password attack** page, enter **Password Spray Test** in the **Name** field and select **Next**.
5. In the **Select user accounts which to attempt the password attack** page, select the **Address Book** button, enter **Lynne** in the **Search** field, select **Lynne Robbins** from the resulting list of users, and then select **Next**.
6. In the **Choose attack settings** page, enter the following list of passwords. Unlike the Brute Force password test, this Spray test allows you to enter all passwords in the field at one time; simply include a space in between each one. Enter the following passwords in the **Password** field: **P@ssw0rd Pa$$w0rd Pa55w.rd**

   Note: You will enter Lynne's actual password on purpose to check the results when a password match occurs. Once you have added all the passwords, select **Next**.
7. In the **Confirmation** page, select **Finish** to run the simulation.
8. Once the attack is complete, you will be returned to the **Attack simulator** page.
9. Leave your browser and the Security and Compliance Center open for the next task.

13.0.4 Task 4: Review the Password Spray results

You will now review the results of the Password Spray attack.

1. In your browser session where you are logged in as Holly Dickson, you should still be on the **Attack simulator** page. In the **Password Spray Attack** section, it should display **Attack Completed** once the attack is done. Select the **Refresh** icon on the address bar to refresh the results. This may take several minutes to complete, so you may need to refresh your screen several times. Once the attack is complete, select **View Report**.
2. On the **Attack details** page, view the report for the **Password spray test** that you completed. Review the information on the page and note the results after having entered Lynne's actual password among the list of passwords that were entered for the simulation.
3. In the **Attack details** page, select **Attack simulator** in the navigation thread at the top of the page (**Home > Attack simulator > Report**).
4. Leave your browser open in LON-CL1 and do not close any of the tabs.

13.0.5 Task 5: Disable Multi-factor Authentication for the Global Admin

To use Microsoft's Attack Simulator to simulate phishing and password attacks, Holly enabled Multi-Factor Authentication (MFA) for her user account. Now that she has completed the Attack Simulator tests, she wants to disable MFA for her account so that she doesn't have to deal with MFA for the remainder of the pilot project.

1. You should still be logged into **LON-CL1** as the **Admin** account and into Microsoft 365 as Holly Dickson.
2. To disable MFA for Holly Dickson's user account, you must first access the **Active users** list in the Microsoft 365 admin center. If you have the **Microsoft 365 admin center** open in a browser tab, then select that now; otherwise, open a new browser tab, enter **https://portal.office.com** in the address bar, and then on the **Office 365 home** page, select **Admin**.
3. On the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users** and then select **Active users**.
4. In the **Active users** window, on the menu bar at the top of the user list, select **Multi-factor authentication**.
5. In the **multi-factor authentication** window, the **users** tab is displayed by default. Select the check box for **Holly Dickson**, and in Holly's properties pane on the right, select **Disable**.
6. On the **Disable multi-factor authentication?** dialog box, select **yes**.
7. When the **Updates successful** dialog box appears, select **close**. In the **multi-factor authentication** window, verify Holly's MFA Status has changed to **Disabled**.
8. You must now sign out of Microsoft 365 as Holly and then sign back in as Holly (without MFA). To do so, perform the following steps:
   - Close your browser session and all browser tabs (to clear your cache)
   - Open a new Edge browser session
   - Enter the **https://portal.office.com** URL
   - Sign in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**
   - From the **Microsoft Office Home** page, select the **Admin** icon to navigate to the **Microsoft 365 admin center**

   You are now ready to proceed to the next lab exercise.

14 Proceed to Lab 3 - Exercise 3

15 Module 3 - Lab 3 - Exercise 3 - Prepare for Alert Policies

Alerts are policies designed to automatically notify administrators when key actions have occurred in their Microsoft 365 tenant. Alerts can be an easy way to ensure that change logs are up-to-date and that business policies are being followed inside your Microsoft 365 tenant.

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment. One of Adatum's business requirements is to set up an alert notification system so that targeted administrators are automatically notified through email when certain actions occur. As you proceed with your Microsoft 365 pilot project, you want to test out Microsoft 365's alert notification system by creating and validating several types of alerts.

There are two requirements to viewing alerts in the Security and Compliance Center – turning on Audit Logging and assigning the proper Role Based Access Control (RBAC) permissions to the users who will view alerts.

- **Audit logging.** If you'll recall, towards the end of Lab 1 you turned on Audit Logging. You performed this task in Lab 1 because it can take an hour or two to propagate that setting through the system before you can successfully implement alerts. So hopefully this propagation completed while you completed the previous modules.
- **RBAC permissions.** In this exercise, you will assign the necessary RBAC role group to Lynne Robbins, who is the user that Holly selected for testing alerts in Adatum's Microsoft 365 pilot project.

15.0.1 Task 1 – Assign RBAC Permissions for Alert Notification Testing

The alerts a user can see on the **View alerts** page is dependent on the assigned RBAC roles, which determine the depth of insight and control a user has. How is this accomplished? The management roles assigned to users (based on their membership in role groups in the Security and Compliance Center) determine which alert categories a user can see on the **View alerts** page (this was covered in the topic on Alerts in the previous module).

For Adatum's pilot project, Lynne Robbins has been selected to test the alert notification system. For Lynne to be able to view alerts and receive alert notifications, she must first be assigned appropriate RBAC permissions in the Security and Compliance Center.

The three alerts that you will create in this lab are assigned to two Alert categories: **Permissions** and **Data Loss Prevention**. The Compliance Data Administrator role group, which includes the Compliance Administrator role, provides permissions for these two alert categories; therefore, assigning Lynne Robbins to this role group will enable her to view the alerts that are created in this lab.

	Data governance	**Data loss prevention**	**Mail flow**	**Permissions**	**Threat M**
Compliance Data Administrator	X	X		X	

Perform the following steps to assign Lynne Robbins the Compliance Data Administrator role group, which includes the Compliance Administrator role.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **Admin** account and into Microsoft 365 as Holly Dickson (**holly@xxxxxZZZZZZ.onmicrosoft.com)** with a password of **Pa55w.rd**.
2. After finishing the previous lab, you should still be in the **Microsoft 365 admin center** in your browser. In the left-hand navigation pane, select **Show all**, and then under the **Admin centers** group, select **Security**.
3. In the **Office 365 Security & Compliance center**, in the left-hand navigation pane, select **Permissions**.
4. On the **Permissions** page, select the **Compliance Data Administrator** role group.
5. In the **Compliance Data Administrator** pane, scroll to the bottom and in the **Members** section, select **Edit**.
6. In the **Editing Choose members** window, select **Choose members**.
7. In the **Choose members** window, select **+Add**, and then in the list of users that appears, select **Lynne Robbins,** and then select **Add.**
8. In the **Choose members** window, select **Done.**
9. In the **Editing Choose members** window, select **Save.**
10. In the **Compliance Data Administrator** window, select **Close.**
11. Leave the Client 1 VM and the Security and Compliance Center tab open for the next task.

You have now added Lynne Robbins to the Compliance Data Administrator role group.

16 Proceed to Lab 3 - Exercise 4

17 Module 3 - Lab 3 - Exercise 4 - Implement Mailbox Permission Alert

In this exercise you will configure and test an alert that will notify Lynne Robbins when FullAccess permissions are granted to any mailbox within Adatum.

17.0.1 Task 1 – Create a Mailbox Permission Alert

1. You should still be logged into your Client 1 VM (LON-CL1) as the **Admin** account and into Microsoft 365 as Holly Dickson (**holly@xxxxxZZZZZZ.onmicrosoft.com)** with a password of **Pa55w.rd**.
2. In the **Office 365 Security & Compliance** center, in the left-hand navigation pane, select **Alerts,** and then under it, select **Alert policies**.
3. In the **Alert policies** window, select **+New alert policy**.
4. In the **New alert policy** window, enter the following information:
   - Name: **Mailbox permission change**
   - Description: **This alert notifies Lynne Robbins when FullAccess permissions are granted to any mailbox in Adatum Corp.**
   - Severity: **Medium**
   - Category: **Permissions**
5. Select **Next.**
6. On the **Choose an activity, conditions and when to trigger the alert** window, enter the following information:
   - Activity is: select the drop-down arrow in the field, enter **mail** in the search box, and select **Granted mailbox permission**
   - How do you want the alert to be triggered? **Every time an activity matches the rule**
7. Select **Next.**
8. On the **Decide if you want to notify people when this alert is triggered** window, enter the following information:
   - Email recipients: Select the "X" to the right of **Holly Dickson's** account to remove her, enter **Lynne**, and then select **Lynne Robbins** from the user list
   - Daily notification limit: **No limit**
9. Select **Next.**
10. Review your settings. When everything is correct, scroll to the bottom of the window and verify the **Yes, turn it on right away** option is selected (select it if necessary) and then select **Finish**.
11. Verify your new alert policy appears in the list on the **Alert policies** page and its **Status** in **On**.
12. Leave the Client 1 VM and the Microsoft 365 admin center and Security and Compliance Center tabs open for the next task.

You have now created an activity alert in the Security & Compliance Center that is triggered when FullAccess permissions are granted to any mailboxes.

17.0.2 Task 2 – Validate the Mailbox Permission Alert

In the prior task, you configured an alert that will notify Lynne Robbins when FullAccess permissions are granted to any mailbox within Adatum. To test this alert, Holly Dickson will change the FullAccess permission on Alex Wilber's mailbox by granting Joni Sherman FullAccess to his mailbox. This activity should trigger

the alert policy that you just created, which should send an alert notification email to Lynne Robbins' mailbox. You will then log into the Client 2 VM as Lynne Robbins and see if she received this email.

1. You should still be logged into the Client 1 VM (LON-CL1) as the **Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, select the **Microsoft 365 admin center** tab, and then in the left-hand navigation pane, under the **Admin centers** group, select **Exchange**. This opens the Exchange admin center for Exchange Online.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **recipients**.
4. In the **recipients** window, the **mailboxes** tab is displayed by default. Select **Alex Wilber** from the list of mailboxes and then select the **pencil (Edit)** icon from the menu bar to edit his mailbox settings.
5. In the **Edit User Mailbox** window, select **mailbox delegation** in the left-hand navigation pane.
6. Scroll down through the **mailbox delegation** page to the **Full Access** section and select the **(+) plus sign** icon.
7. In the **Select Full Access** window, select **Joni Sherman**, select the **add ->** button, and then select **OK**.
8. In the **Edit User Mailbox** window, select **Save**, and then select **OK** once the information is saved.
9. Since **Holly Dickson** has changed the mailbox permissions for Alex Wilbur by giving Joni Sherman FullAccess permissions to his mailbox, an alert email should automatically be sent to Lynne Robbins' Inbox that notifies her of this event.

   Switch to LON-CL2.
10. In your Edge browser, select the **Mail - Lynne Robbins - Outlook** tab that has Outlook on the web open for Lynne Robbins' mailbox. In Lynne Robbins' **Inbox**, an email should be received from the Alerts notification system (**Office365Alerts@microsoft.com**) to let her know that Holly Dickson has made a Mailbox permission change.

    Note: In can take up to 15 minutes or so for the email to be received in Lynne's Inbox.
11. Open the email and review the contents. Scroll to the bottom of the email and select the **View alert details** button. This opens the **Security and Compliance Center**, displays the **View alerts** window, and opens the **Mailbox permission change** alert.

    Scroll down through the **Mailbox permission change** alert and review all the information. When you are done, select **Close** to close the **Mailbox permission change** alert, then close the **View alerts** tab in your browser.
12. Switch back to the LON-CL1.
13. In the **Microsoft 365 Security & Compliance center**, in the left-hand navigation pane, select **Alerts,** and then under it, select **View Alerts**. The notification that was just created based on the **Mailbox permission change** alert should appear in the list.
14. In your browser, close the Exchange admin center tab (**mailboxes - Microsoft Exchange**), but leave the other browser tabs open.
15. Leave your LON-CL1 and LON-CL2 VMs open for the remaining tasks in this lab.

You have just successfully tested a mailbox permission alert that sent an alarm message on granting FullAccess to a user mailbox.

18 Proceed to Lab 3 - Exercise 5

19 Module 3 - Lab 3 - Exercise 5 - Implement SharePoint Permission Alert

In this exercise you will configure and test an alert that notifies Lynne Robbins when a user is added to the site collection administrators for a SharePoint site collection.

19.0.1 Task 1 – Create a SharePoint Permissions Alert

1. You should still be logged into the Client 1 VM (LON-CL1) as the **Admin,** and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, in the **Office 365 Security & Compliance** center, in the **Alerts** section in the left-hand navigation pane, select **Alert policies**.
3. In the **Alert policies** window, select the **+New alert policy** button.
4. In the **New alert policy** window, enter the following information:
   - Name: **Site collection admin permissions**
   - Description: **This alert notifies Lynne Robbins when a user is added to the site collection administrators on a SharePoint site collection.**
   - Severity: **Medium**
   - Category: **Permissions**
5. Select **Next.**
6. On the **Choose an activity, conditions and when to trigger the alert** window, enter the following information:
   - Activity is: select the drop-down arrow in the field, enter **site collection** in the search box, and select **Added site collection admin**
   - How do you want the alert to be triggered? **Every time an activity matches the rule**
7. Select **Next.**
8. On the **Decide if you want to notify people when this alert is triggered** window, enter the following information:
   - Email recipients: Remove **Holly Dickson** and add **Lynne Robbins**
   - Daily notification limit: **No limit**
9. Select **Next.**
10. Review your settings. When everything is correct, verify the **Yes, turn it on right away** option is selected and then select **Finish**.
11. Leave the Client 1 VM and the Microsoft 365 admin center and Security and Compliance Center tabs open for the next task.

You have now configured an additional alert policy that monitors when a site collection administrator is added to SharePoint Online site collections.

19.0.2 Task 2 – Validate the SharePoint Permissions Alert

In the prior task, you configured an alert that will notify Lynne Robbins when a site collection admin is added to a site collection. To test this alert, Holly Dickson will add Alex Wilber as a site collection admin to the global SharePoint Communication site. This activity should trigger the alert policy that you just created, which should send an alert notification email to Lynne Robbins' mailbox. You will then switch to the Client 2 VM to see if Lynne received this email.

1. You should still be logged into the Client 1 VM (LON-CL1) as the **Admin**, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, open a new tab and enter the following URL in the address bar: **https://xxxxxZZZZZZ.sharepoint.com/_layouts/15/settings.aspx** (replace xxxxxZZZZZZ with the tenant prefix provided by your lab hosting provider). This opens the **Site Settings** for the global SharePoint Communication site.
3. On the **Site Settings** window, under the **Users and Permissions** section, select **Site permissions**.
4. In the ribbon at the top of the page, the **Permissions** tab is displayed by default. Under the **Manage** group, select **Site Collection Administrators**.

5. In the **Site Collection Administrators** dialog box, the Company Administrator is displayed by default in the data entry field. To the right of Company Administrator, enter **Alex**, select **Alex Wilber** from the list of users that appears, and then select **OK**.
6. Since a new site collection admin has been added, an alert should automatically be sent to Lynne Robbins' Inbox notifying her of this event. Perform the remaining steps to verify that Lynne received this email.

   Switch to the Client 2 VM (LON-CL2).
7. From the prior task, you should still be logged into **Outlook on the web** as **Lynne Robbins**. Monitor Lynne's Inbox to view the email generated by the alert that you just created.

   Note: Based on lab testing, the time for an email to be generated and received in Lynne's Inbox can range from a couple of minutes to an hour.
8. Once the email arrives in Lynne's Inbox, open the email and review the contents. Scroll to the bottom of the email and select the **View alert details** button. This opens the **Office 365 Security and Compliance** center, displays the **View alerts** window, and opens the **Site collection admin permissions** alert.

   Scroll down through the alert and review all the information. When you are done, select **Close** to close the alert, then close the **View alerts** tab in your browser.
9. Switch back to the LON-CL1.
10. In the **Office 365 Security & Compliance** center, in the left-hand navigation pane under the **Alerts** section, select **View Alerts**. The notification that was just created based on the **Site collection admin permissions** alert should appear in the list.
11. Leave your LON-CL1 and LON-CL2 VMs open for the remaining tasks in this lab.

You have now successfully tested the SharePoint alert to monitor site collection admin permissions on SharePoint sites.

20 Proceed to Lab 3 - Exercise 6

21 Module 3 - Lab 3 - Exercise 6 - Test the Default eDiscovery Alert

In this exercise you will test a default Microsoft 365 alert policy that notifies all tenant admins, such as Holly Dickson, whenever an eDiscovery search has been created or exported.

Note: Creating an eDiscovery alert of this nature is important because an eDiscovery search, when left unregulated, can pull sensitive content that can be exported to an unauthorized source.

21.0.1 Task 1 – Review the default eDiscovery Alert

In this task, you will verify whether a default Microsoft 365 alert is triggered when somebody in your tenant creates an eDiscovery search or exports data from an existing search. Since Holly Dickson is assigned the Global Admin role, she is automatically a member of the Tenant Admins and will be one of the recipients of this alert.

1. You should still be logged into the Client 1 VM (LON-CL1) as the **Admin,** and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, select the **Office 365 Security & Compliance** center tab.
3. In the **Office 365 Security & Compliance** center, the **Alert policies** window should still be open from the prior task; if not, select **Alerts** and then **Alert Policies** from the left-hand navigation bar.
4. You want to search through the default system policies for a policy named **eDiscovery search started or exported**. Since there are so many pre-existing system policies, the easiest way to locate the policy is to search for it. In the **Search** field at the top of the screen, enter **eDiscovery**. In the policy list, you should see **eDiscovery search started or exported**. Select the check box next to this policy.
5. An **eDiscovery search started or exported** pane should appear. Scroll down through **eDiscovery search started or exported** pane and verify the settings are configured as follows:
   - Status: **On**
   - Conditions: **Activity is eDiscoverySearchStartedOrExported**
   - Aggregation: **Single event**

- Scope: **All users**
- Email recipients: **TenantAdmins**

6. If all settings are correct, select the **Close** button to close the **eDiscovery search started or exported** pane.
7. In the **Alert policies** list, select the **ellipsis** icon that appears on the far right side of **eDiscovery search started or exported** row, and then in the menu that appears, select **Edit**.
8. An **Edit recipients** pane appears. This window enables you to edit the email recipients who are notified when this policy is triggered. You will not change the value here; instead, the purpose of this step is to show you how to change the recipient list in your real-world implementations for any of the default system policies. Select **Close**.

You have now reviewed the default Microsoft 365 eDiscovery alert that notifies tenant admins when an eDiscovery search is created or exported.

21.0.2 Task 2 – Validate the default eDiscovery Alert

To test this default alert, Holly Dickson will create an eDiscovery search. This activity should trigger the alert policy, which should send an alert notification email to all Tenant Admins. Holly is a Global admin, who by default are members of the Tenant Admin group; therefore, she should receive the email notification generated by this alert.

1. You should still be logged into the Client 1 VM (LON-CL1) as the **Admin,** and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, select the **Office 365 Security & Compliance** center tab.
3. In the **Office 365 Security & Compliance** center, in the left-hand navigation pane, select **Search**, and then under it, select **Content search**.
4. The **Content search** window has two tabs - a **Searches** tab and an **Exports** tab. The **Searches** tab is displayed by default. Select the **+New search** button.
5. In the **Search query** pane that appears, enter **Confidential** in the **Enter keywords** field.
6. In the **Locations** section, select the **Specific locations** option and then select **Modify**. This opens the **Modify locations** window. There are three groups of locations, each of which can be turned On or Off through its respective toggle switch. Turn the toggle switch **On** (if necessary) for the first group, but leave the toggle switches **Off** for the other two. At least one group must be set to **On**; otherwise, you will receive an error. Select **Save**.

   Note: While you could have simply selected the **All locations** option, you were asked to select a specific set of locations just so that you could see all the various locations that can possibly be searched in an eDiscovery search.
7. Select **Save & run**. In the **Save search** pane that appears, enter **Confidential search** in the **Name** field and then select **Save**.

   Important: When you save a new search, the system saves the search and then immediately runs it. By saving this eDiscovery search, the eDiscovery alert should be triggered, thereby creating an email notification that should be sent to the Inbox of all users with tenant admin permissions. You do NOT have to wait for the Search to finish before testing whether the alert sent the email notification. The alert notification system will process the email at the time the search is saved.

   Do NOT wait for the search to finish. Proceed to the next step.
8. For the purpose of this lab, you should cancel the search to remove the overhead from your limited system resources. The screen should currently indicate that it is **Searching**. Select the **Cancel** button to stop the search, and then select **Yes** to confirm the cancellation. Canceling the search takes a minute or so to complete.
9. To test this alert, open a new tab in your browser and go to **Outlook on the web** by entering the following URL in the address pane: **https://outlook.office365.com**
10. When Outlook opens, if the language and time zone window appears, select your Language and Time zone and select **Save**.

11. Monitor Holly's Inbox for the email that was automatically sent by the Alerts notification system to inform her that an eDiscovery search was created or exported. Once the email is received, open it and review the contents, then close the message.

    Note: It may take up to 10 minutes or so before the email arrives in Holly's Inbox.

12. In your **Edge** browser, switch back to the **Office 365 Security & Compliance** center tab and under the **Search** group in the left-hand navigation pane, select **Audit Log Search**.

13. At the bottom of the page, select the **Search** button to display all recent activity. This will display the activity that created this alert.

    Note: In the list of search results, note how the **User** for the prior alerts is listed as Holly, while the user for the eDiscovery alert is listed as **Service Account**. This is because the eDiscovery alert is a default system alert rather than a custom alert created by an individual user.

14. In your browser, leave the Outlook tab (**Mail-Holly Dickson - Outlook**) open as you will use it shortly in another lab exercise. Leave all your other browser tabs open as well.

You have now successfully tested the Microsoft 365 eDiscovery system alert that monitors the creation of an eDiscovery search or the export of data from a completed search.

22 End of Lab 3

23 Module 4 - Lab 4 - Exercise 1 - Configure Office 365 Message Encryption

In this lab, you will take on the persona of Holly Dickson, Adatum's Enterprise Administrator. You have been tasked with piloting the use of Microsoft 365 message encryption in Adatum's Microsoft 365 deployment. Since message encryption rules can be created using both Exchange Online and Windows PowerShell, you have decided to test each method to determine which you prefer to use once you go live.

In this exercise you will set up Azure Rights Management Services (RMS) for your tenant. You will also learn how to create a mail flow encryption rule using both the Exchange Admin Center and Windows PowerShell.

23.0.1 Task 1 – Enable Azure Rights Management for Exchange Online

In this task you will use Windows PowerShell to access Exchange Online and then, through a string of commands, you will confirm that Azure RMS is active.

1. You should still be logged into LON-CL1 as **Admin**, and you should still be logged into Microsoft 365 as **Holly Dickson**.

2. To open Windows PowerShell, enter **powershell** in the **Search** box on the taskbar.

3. In the menu that appears, right-click on **Windows PowerShell** and select **Run as administrator** in the drop-down menu.

4. In **Windows PowerShell**, you must begin by installing the **Microsoft Azure Active Directory Module for Windows PowerShell** by running the following command at the command prompt:

   Install-Module MSOnline

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

6. 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.**

7. Once the installation is complete, the screen will return to the command prompt. You must then run the following command to initiate a connection to Azure Active Directory:

   Connect-MsolService

8. A new window will appear requesting your credentials. Sign in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**.

9. Running unsigned PowerShell scripts from remote computers requires changing the execution policy for PowerShell. You should run the following command that changes the Execution Policy for this PC to **unrestricted**, which sets access to the external authorization for this PC so that it can connect to Microsoft online and load all configuration files and run all scripts:

   Set-ExecutionPolicy unrestricted

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

11. You must then run the following command to prompt for the username and password of the user who will be running any subsequent commands; this set of credentials will be stored in the $Cred macro:

    $Cred = Get-Credential

12. A **Windows PowerShell credential request** window will appear. Sign in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and a password of **Pa55w.rd**.

13. You must then run the following command to create a PSSession (titled $Session) that establishes a remote connection to Exchange Online through PowerShell. When you create a PSSession, Windows PowerShell establishes a persistent connection to the remote computer. Without the -Credential parameter that invokes the $Cred macro from the prior step, this command would prompt you for the credentials of the user authorizing this command. In this case, by invoking the $Cred macro, it applies Holly's username and password.

    $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $Cred -Authentication Basic -AllowRedirection

    Note: It's important to note that you must connect to Exchange Online PowerShell with an admin account that cannot be enabled for multi-factor authentication (MFA). In a real-world environment, if your admin account is enabled for MFA, you must install the Exchange Online Remote PowerShell Module and use the **Connect-EXOPSSession** cmdlet to connect. For more information, see the following article on how to Connect to Exchange Online PowerShell using multi-factor authentication.

14. You should then run the following cmdlet to import commands, such as cmdlets, functions, and aliases, from the PSSession ($Session) created in the prior step. In this case, it imports the Exchange Online session into the PowerShell GUI.

    Import-PSSession $Session

    Note: You can ignore the warning message that is displayed regarding unapproved verbs.

15. You must then run the following command to view the Information Rights configuration for Exchange Online:

    Get-IRMConfiguration

16. To validate whether Azure Rights Management Services is enabled, scroll through the list of parameters that's displayed and locate the **AzureRMSLicensingEnabled** parameter. If this value is set to **$true**, then Azure RMS is turned On and you can proceed to the next step.

    Important: If **AzureRMSLicensingEnabled** is set to **$false**, then you must run the following command to turn on Azure RMS before you can proceed to the next step:

    Set-IRMconfiguration -azureRMSLIcensingEnabled $true

17. Now that Azure RMS is enabled, you should run the **Test-IRMConfiguration** cmdlet to test Information Rights Management (IRM) configuration and functionality, including availability of an Active Directory RMS server, pre-licensing, and journal report decryption. To perform this test, run the following command to test the IRM configuration for messages sent from Holly Dickson:

    Test-IRMConfiguration -Sender Holly@xxxxxZZZZZZ.onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)

    Note: The results should appear as follows:

    Results: Acquiring RMS Templates ...

    ```
    - PASS: RMS Templates acquired. Templates available: Confidential \ All Employees, Highly Confiden
    All Employees, Encrypt, Do Not Forward.
    ```

Verifying encryption ...

```
- PASS: Encryption verified successfully.
```

Verifying decryption ...

```
- PASS: Decryption verified successfully.
```

Verifying IRM is enabled ...

```
- PASS: IRM verified successfully.
```

OVERALL RESULT: PASS

18. Leave your PowerShell window open as you will return to it in a later task; simply minimize the PowerShell window for now.

23.0.2 Task 2 – Create a Mail Flow Encryption Rule using the Exchange admin center

In this task, you will create an encryption rule for messages inside your Exchange Online environment by using the Exchange admin center. In the next task, you will do the same thing but using PowerShell instead.

1. On the LON-CL1 VM, you should still be logged into the **Microsoft 365 admin center** as **Holly Dickson**. If you closed your Edge browser or the **Microsoft 365 admin center** tab, then in your Edge browser navigate to **https://portal.office.com**, sign in as **Holly@xxxxxZZZZZZ.onmicrosoft.com**, and select **Admin**.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all** (if necessary), and then under **Admin centers**, select **Exchange**. This will open the Exchange admin center.
3. In the **Exchange admin center**, in the left-hand navigation pane select **mail flow.**
4. At the top of the **mail flow** page, the **Rules** tab is displayed by default. In the **Rules** tab, select the **plus sign** (+) icon to create a new rule. This displays a drop-down menu of actions. Select **Create a new rule.**
5. In the **new rule** window, in the **Name** box, enter **Encrypt mail for guest@adatum.com** as the name of this rule.
6. Select the drop-down arrow in the **Apply this rule if…** condition box. In the drop-down menu, select **the recipient is**.
7. For this condition, you must either select an existing name from the user list or type a new email address in the **check names** box. In this case, enter **guest@adatum.com** in the **Check names** box and then select **OK**.
8. You need to add more conditions, so scroll down (if necessary) and select **More options**.
9. Select **add condition**.
10. Note how a second condition box appears below **The recipient is...** condition box. In this second condition box, select the drop-down arrow and select **The recipient**. Then in the drop-down menu select **is external/internal.**
11. In the **select recipient location** dialog box, select the drop-down arrow. In the drop-down menu, select **Outside the organization** and then select **OK.**
12. You now need to define an action to perform when this rule is applied. In the **Do the following...** box, select the drop-down arrow. In the drop-down menu, hover your mouse over **Modify the message security...** and in the menu that appears, select **Apply Office 365 Message Encryption and rights protection.**
13. In the **select RMS template** dialog box, select the drop-down arrow, select **Encrypt**, and then select **OK.**
14. Select **Save.** Once the rule is saved, it should appear in the list of rules in the Exchange admin center.
15. Leave your browser tabs open and proceed to the next task.

23.0.3 Task 3 – Create a Mail Flow Encryption Rule using Windows PowerShell

In a prior task, you configured a mail flow encryption rule using the Exchange admin center. In this task, you will create a mail flow encryption rule using Windows PowerShell.

1. On the LON-CL1 VM, the PowerShell session that you used in the prior task should still be open. Select the PowerShell icon on the taskbar.

   Important: If you closed the previous PowerShell session, then repeat steps 1-14 from Task 1 to create a PSSession that establishes a remote connection to Exchange Online through PowerShell and then imports the Exchange Online session into the PowerShell GUI. This is required because the New-TransportRule cmdlet used in the next step does not exist in MsolService because it is an Exchange Online cmdlet; therefore, you must connect to the Exchange Online session through PowerShell to access this cmdlet.

2. In this step, you will create a mail flow rule by using the **New-TransportRule** cmdlet, and you will set the **ApplyOME** encryption parameter to $true. This rule will encrypt all outgoing mail from Adatum that is being sent to Gservices@adatum.com.

   To create this rule, run the following command:

   New-TransportRule -Name "Encrypt rule for Guest Services" -SentTo "Gservices@contoso.com" -SentToScope "NotinOrganization" -ApplyOME $true

   Note: This command will take several seconds to complete.

3. To verify the rule exists, minimize your PowerShell window. In your Internet Explorer browser session, you should still be in the **mail flow** window of the **Exchange admin center**, and the **rules** tab should be displayed. The list of rules should only display the **Encrypt mail for guest@adatum.com** rule that you created in the prior task.

   On the menu bar that appears above the list of rules, select the **Refresh** icon. In the refreshed list, the rule that you just created using PowerShell should appear as well.

4. Leave your browser session open for the next exercise.

24 Proceed to Lab 4 - Exercise 2

25 Module 4 - Lab 4 - Exercise 2 - Validate Information Rights Management

In this exercise, you will learn how to validate Information Rights Management for both Exchange Online and SharePoint Online.

25.0.1 Task 1 - Validate Information Rights Management for Exchange Online

In the prior exercise, you set up Information Rights Management in Exchange Online for Adatum. In this exercise, you will validate that configuration by sending a protected email from Holly Dickson to Alex Wilber. You will then log into Alex's mailbox on the Client 2 VM (LON-CL2), open the email, and verify that it's protected.

1. On the Client 1 VM (LON-CL1), you should still be logged into the Microsoft 365 admin center as Holly Dickson.
2. In the earlier exercise in which you created an eDiscovery alert, you opened **Outlook on the web** for Holly. This tab should still be open in your browser, so select it now; however, if you closed Outlook, then open a new tab in your browser and enter the following URL: **https://outlook.office365.com**
3. At the top of the left-hand navigation pane, select **+New message** to create a new email.
4. You want to send the email to **Alex Wilber**. Type **Alex** in the **To** field and select **Alex Wilber** from the list of users that are displayed.
5. Enter **IRM test** in the **Subject** line and then enter some text in the message body.
6. In the menu bar above the message pane, select **Encrypt** (this option appears because you set up IRM in Exchange in the prior task).

7. This displays a message below it that indicates the message is encrypted. In this message box, select **Change permissions**, which opens a **Change permissions** dialog box.
8. In the **Change permissions** dialog box, in the **Choose how recipients can interact with this message** field, select the drop-down arrow, select **Do not forward**, and then select **OK**.
9. Select **Send** to send the email to Alex.
10. Switch to the Client 2 VM (LON-CL2).
11. If you need to log in as the **Admin** account, then do so with a password of **Pa55w.rd**.
12. In an earlier lab exercise, you opened **Outlook on the Web** on LON-CL2 for Lynne Robbins. You must log out as Lynne so that you can sign back in as Alex.

    Select Lynne's user icon in the upper right corner, and in her **My account** window, select **Sign out**. Once you are signed out, close all tabs in your browser except for the **Sign out** tab.
13. In your **Edge** browser, in the **Sign out** tab, enter the following URL in the address bar: **https://outlook.office365.com**.
14. In the **Pick an Account** window, only Lynne's account and the MOD Administrator's account appear. Select **Use another account** and log in as **AlexW@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with a password of **Pa55w.rd**.
15. Close the **Welcome** window that appears.
16. In Alex's **Inbox**, verify that he received the email that you sent from Holly that is IRM protected. IRM protected emails display a lock icon to the right of the message. Select the message to display it in the right-hand pane.
17. You should see a message at the top of the message pane that says **This message is encrypted and recipients can't forward it.** A lock icon should appear next to this message as well, which indicates the message is encrypted.
18. In the message pane for this email, note how the **Forward** arrow is disabled. Similarly, at the bottom of the email, note how the **Reply** option is enabled, but the **Forward** option is not.
19. In the message pane for this email, select the **ellipsis (More actions)** icon that appears to the right of the disabled Forward arrow. In the drop-down list that appears, note how the **Print** option is disabled. Encrypted emails can neither be forwarded or printed.
20. You want to remain logged into the Microsoft 365 as Alex Wilber on LON-CL2 for the next task, so leave your browser tabs open and proceed to the next task.

25.0.2 Task 2 - Validate Information Rights Management for SharePoint Online

In Lab 1, you enabled Information Rights Management for Adatum in SharePoint Online. Ideally, you would have enabled IRM for SharePoint Online at the start of this exercise, just as you did when enabling IRM for Exchange Online. However, since it can take an hour or more for IRM to show up in SharePoint Online once it's enabled, that task was moved to Lab 1 so that by the time you got to this task, IRM would be ready for you in SharePoint.

You will begin by having Holly create a new SharePoint site collection. You will then configure it for Information Rights Management, share it with Alex Wilber, and then have Alex validate IRM for the site.

1. Switch to the LON-CL1 VM where you should still be logged into the **Microsoft 365 admin center** as **Holly Dickson**.
2. In the **Microsoft 365 admin center**, scroll down through left-hand navigation pane and under **Admin centers**, select **SharePoint**. This will open the SharePoint admin center in a new browser tab.
3. In the **SharePoint admin center**, in the left-hand navigation pane, select **Sites** and then select **Active sites**.
4. In the **Active sites** window, select **+Create** on the menu bar.
5. On the **Create a site** pane that appears, you must choose the type of site you want to create. Select the **Team site** tile.
6. On the **Get a team site connected to Microsoft 365 Groups** pane, enter the following information:

- Site name: **Marketing**
- Group email address - **Marketing** is filled in automatically after entering the Site name; leave as is
- Site address - **Marketing** is filled in automatically after entering the Site name; leave as is
- Group owner: Enter **Holly**, and then in the list of users that is displayed, select **Holly Dickson**
- Select a language: select your language

7. Select **Advanced settings** and then enter the following information:
   - Privacy settings: **Private - only members can access this site**
   - Time zone - select your time zone
8. Select **Next**.
9. On the **What do you want to add?** pane, enter **Alex** in the **Add members** field and then select **Alex Wilber** from the list of users. Select **Finish**.
10. If the new **Marketing** site collection does not appear in the **Site Collections** list after a couple of minutes, select the **Refresh** icon to the left of the address bar. If it still doesn't appear, wait another minute or two and refresh the list again. Continue until the new site collection appears.
11. You will now open the new SharePoint site that you just created. In your web browser, open a new tab and enter the following URL in the address bar: **https://xxxxxZZZZZZ.sharepoint.com/sites/marketing** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)
12. On the **Marketing** site, in the left-hand navigation pane, select **Documents.**
13. In the **Documents** page for the **Marketing** site, at the top right of the title bar, select the **gear (Settings)** icon and then in the **Settings** drop-down menu that appears, select **Library settings**. Note - it may take a minute or two for the gear icon to appear.
14. On the **Documents > Settings** page, in the **Permissions and Management** column, select **Information Rights Management**.
15. On the **Settings > Information Rights Management Settings** page, select the **Restrict permissions on this library on download** check box.
16. In the **Create a permission policy title** field, enter **Marketing Policy**.
17. In the **Add a permission policy description** field, enter **Marketing policy for downloads**.
18. Select **SHOW OPTIONS**.
19. In the **Configure document access rights** section, select the **Allow viewers to write on a copy of the downloaded document** check box and then select **OK**.
20. On the **Documents > Settings** page, select the **Documents** portion of this page title. This returns you to the **Documents** page for the **Marketing** site.
21. On the **Documents** page, select the **gear (Settings)** icon and then in the **Settings** drop-down menu that appears, select **Site permissions**.
22. In the **Permissions** pane that appears, select **Site members** and note that only the **Marketing Members** have permission to access the Documents site.
23. To share this Documents site with Alex Wilber, in the **Permissions** pane select the **Invite people** button. In the drop-down menu that appears, select **Share site only**.
24. On the **Share site** pane, enter **Alex** in the field, then select **Alex Wilber** from the user list, verify the **Send email** check box is selected (if not, select it now), and then select **Add**.
25. In the **Permissions** pane, select **Site members** and note that **Alex Wilber** is now included along with the **Marketing Members**.
26. Close the **Permissions** pane.
27. Select the **Start** icon in the bottom left corner of the taskbar, and then in the Program menu, select **Microsoft Word**.
28. When **Microsoft Word** opens, select **Blank document**.

29. Enter some text in the document, then save the file to the **Desktop** as whatever file name you wish.
30. Close Word.
31. Since Holly has her Outlook mailbox open, she is simply going to email the file that she just created to Alex. Select the **Outlook on the Web** tab in your browser that contains Holly's mailbox that you just used in the prior task when you emailed Alex.
32. Send an email to Alex Wilber and attach the file that you just created and stored on the Desktop.
33. Now that Holly has created this new SharePoint site and used IRM to restrict permissions on the site, she has asked Alex Wilber to test this site to validate whether IRM is working for SharePoint Online. Alex will perform this test on the Client 2 (LON-CL2) VM.

    Switch to the **LON-CL2** VM, where you should still have **Outlook on the Web** open in your **Microsoft Edge** browser from the prior task. You should still be logged in as **Alex Wilber**.
34. In the **Outlook on the Web** tab, open the email that you just received from Holly that contains the file Holly created earlier. Save the file to the **Documents** folder on your **C** drive.
35. In the browser, open a new tab and enter the following URL in the address bar to navigate directly to the Marketing site: **https://xxxxxZZZZZZ.sharepoint.com/sites/marketing** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider)
36. If a **We've got a new look** window appears, select **NOT NOW**.
37. On the **Marketing** site, select **Documents** on the left-hand pane.
38. On the **Documents** page, in the menu bar, select **Upload**, and then in the drop-down menu select **Files**.
39. In the **File Explorer** window, navigate to the **Documents** folder, which is where you saved the file that Holly emailed to Alex a few steps ago. Select the file and then select **Open**.

    This will upload the file to the **Documents** page in the **Marketing** site collection.
40. In the list of Documents, right-click on the file that you just uploaded, select **Open** in the menu that appears, and then select **Open in browser**.
41. In Word Online, if a **Your privacy option** window appears, then close it. Verify that a warning message appears at the top of the page indicating a **Marketing policy for downloads** applies to the file.
42. Try to enter some text in the document. Verify that Alex cannot edit the document in Word Online because it's protected in this site collection. A **Read-only** information line will display at the top of the page indicating the document is read-only.

    You have just verified that the Marketing site collection is protected by SharePoint Information Rights Management. The document that Alex just uploaded to the SharePoint Online site is flagged as read-only and cannot be updated.
43. Leave your browser open for the next lab; do not close any of the tabs.

26 End of Lab 4

27 Module 5 - Lab 5 - Exercise 1 - Initialize Compliance

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, your next steps are to implement archiving and retention at Adatum. You will begin by initializing compliance through the MDM auto-enrollment of new devices in your tenant. You will then configure retention tags and policies, and you will implement archiving with MRM retention tags.

27.0.1 Task 1 - Create a Group for Compliance Testing

To test archiving and retention in your Adatum pilot project, you will create a new mail-enabled security group and assign two users to the group – Joni Sherman and Lynne Robbins. These will be your two test users involved in the Windows Information Protection (WIP) pilot program. This group will then be used in the next task when you configure MDM auto-enrollment for new devices in your tenant.

1. At the end of the prior lab, you were using the LON-CL2 VM. Switch to the **LON-CL1** VM.

   You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.

2. In **Microsoft Edge**, select the **Microsoft 365 admin center** tab; if you closed this tab earlier, then open a new tab and go to **https://admin.microsoft.com.**

   At this point, you probably have quite a few tabs open in your browser. If you wish, you can take this opportunity to close every tab except for the **Office 365 Home** tab and the **Microsoft 365 admin center** tab.

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

4. On the **Active groups** window, select **Add a group** to create a new group for compliance testing.

5. In the **Add a group** window, adding a group is a multi-step process, as depicted in the flow diagram on the left-hand side of the window. As you progress through the steps, enter the following information to create a new group:

   - Type: **Mail-enabled security**
   - Name: **WIP Users** (tab into the **Description** field to enable the **Next** button)
   - Group email address: **wipusers**
   - Group email address domain: to the right of the group email address alias is the email address domain. **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) should be displayed here. Select this field so enable the **Next** button but do not change its value.

6. On the **Review and finish adding group** window, select **Create group**. Once the group is created, note the warning at the top of the **New group created** window that indicates it can take up to an hour for the group to appear in the Groups list. Our testing experience has shown that the group normally appears within a few minutes.

7. On the **New group created** window, select **Close**.

8. This will return you to the **Active groups** list in the **Microsoft 365 admin center**. Select the **Refresh** icon on the menu bar to refresh the list of groups. You cannot proceed until the WIP Users group appears in the list; therefore, keep refreshing the list every minute or so.

9. Once **WIP Users** appears In the **Groups** list, select it.

10. In the **WIP Users** pane that appears, select the **Members** tab.

11. In the **Members** tab, in the **Members** section select **View all and manage members**.

12. In the **View members** window, select the **+Add members** button; this displays the list of users.

13. In the list of users, select **Joni Sherman** and **Lynne Robbins**, select **Save**, and then select **Close**.

    Note: It may take a few minutes for both Joni and Lynne to display in the list of users. Simply refresh the list until both users appear.

14. In the **WIP users** window, select **Close**.

15. Leave your browser open to the Microsoft 365 admin center and proceed to the next task.

27.0.2 Task 2 – Configure Mobile Device Management (MDM) Auto-enrollment

In this task you will activate MDM auto-enrollment for new devices in your Adatum Corporation tenant. The devices will belong to members of the WIP Users group that you created in Azure AD in the prior task. Activating MDM auto-enrollment is required so that you can implement Windows Information Protection in a later lab. You will also verify that Intune is set by default as your mobile device management authority.

1. You should still be in LON-CL1 and logged into Microsoft 365 as Holly Dickson.

2. In the **Microsoft 365 admin center** tab in your browser, in the left-hand navigation pane, select **Show all** (if necessary), and then in the **Admin centers** section, select **Azure Active Directory**.

3. In the **Azure Active Directory admin center**, select **Azure Active Directory** in the left-hand navigation pane.
4. This returns the **Adatum Corporation | Overview** page. Under the **Manage** section in the middle pane, scroll down and select **Mobility (MDM and MAM)**.
5. In the right-hand pane, select **Microsoft Intune**.
6. This returns the **Configure** window, from which you can configure MDM and MAM settings for Microsoft Intune. For the **MDM User scope** option, select **Some.** This will display a **Groups** option below the **MDM user scope** option.
7. To the right of the **Groups** option, select **No groups selected**.
8. In the **Select groups** pane that appears, scroll down through the list of groups, select **WIP Users**, and then at the bottom of the pane select the **Select** button.

   Note: You configured the **MDM user scope** to automatically enroll devices that belong to members of the **WIP Users** group into MDM management with Microsoft Intune. Once Holly tests this feature in Adatum's pilot project, and assuming she is satisfied with the results, she will then set the **MDM user scope** to **All**.
9. This returns the **Configure** window. In the middle pane, select **Restore default MDM URLs** to ensure the correct URLs are set.
10. Select **Save** on the menu bar at the top of the page.
11. Select the **Microsoft 365 admin center** tab in your browser. In the left-hand navigation pane, under the **Admin centers** section, select **Endpoint Manager**.
12. In the **Microsoft Endpoint Manager admin center** window, select **Tenant administration** in the left-hand navigation pane.
13. In the **Tenant admin | Tenant status** page, verify the **MDM authority** is set to **Microsoft Intune**.
14. In your Microsoft Edge browser, you can close the Endpoint Manager admin center tab and the Azure Active Directory admin center tab. Leave the Microsoft Office Home tab and the Microsoft 365 admin center tab open.

You have configured automatic enrollment in Intune for devices of users in the WIP Users group, and you have verified the MDM authority for Adatum's tenant is set to Microsoft Intune.

28 Proceed to Lab 5 - Exercise 2

29 Module 5 - Lab 5 - Exercise 2 - Configure Retention Tags and Policies

In this exercise, you will implement archiving with MRM retention tags. You will then configure retention tags and policies through two different ways - first, through the Exchange Admin Center, and second, through the Security and Compliance Center.

29.0.1 Task 1 – Activate In-Place Archiving

In this next phase of your Adatum pilot project, you will access the Security & Compliance Center to activate Holly Dickson's archive mailbox.

1. You should still be logged into LON-CL1 as the **Admin** and into **Microsoft 365** as Holly Dickson.
2. In Microsoft Edge, in the **Microsoft 365 admin center**, under the **Admin centers** group, select **Compliance** to open the Office 365 Security and Compliance center.
3. In the **Microsoft 365 Compliance** center, in the left-hand navigation pane, select **Information governance**, and then under it select **Archive**.
4. On the **Archive** window, note that the archive mailboxes for all users other than Holly Dickson are **enabled**. These archive mailboxes were enabled when the VM lab environment was built for this training course and these users were preconfigured in the tenant. However, since Holly's user account was added in Lab 1, her archive mailbox is **disabled** by default.

5. To enable Holly's archive mailbox, click on the checkbox near **Holly Dickson** in the user list and select **Enable Archive** in the tools line.
6. In the **Warning** dialog box that appears, select **Enable** to confirm this action.
7. In your Microsoft Edge browser, leave the Office 365 Compliance Center tab open as you will use it in a later task in this lab.

29.0.2 Task 2 – Create an MRM retention tag and policy in the Exchange Admin Center

As part of your pilot project for Adatum, you will configure MRM retention through the Exchange Admin Center by creating an MRM retention tag and then adding it to a new MRM retention policy. You will also assign several default tags to the policy as well. You will then assign this retention policy to Joni Sherman and Lynne Robbins' mailboxes.

1. On LON-CL1, select the **Microsoft 365 admin center** tab in your Edge browser.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane under the **Admin centers** group, select **Exchange**. This will open the Exchange admin center.
3. In the **Exchange admin center**, in the left-hand navigation pane, select **compliance management**.
4. In the **compliance management** window, in the list of tabs that appear across the top of the page, select **retention tags**.
5. You want to create a retention tag, so select the **plus (+) sign** icon in the toolbar that appears above the list of existing retention tags. In the drop-down menu that appears, select **applied by users to items and folders (personal)**.
6. In **new tag applied by users to items and folders (personal)** window, enter **3 Years Move – Archive after three years** in the **Name** field.
7. Under **Retention Action**, select the **Move to Archive** option.
8. Under **Retention period**, select the **When the item reaches the following age (in days)** option and enter **1095** in the retention period field that appears below this option (1095 days = 3 years).
9. In the **Comment** field, enter **Personal tag to archive email three years after being received**.
10. Select **Save** to save the retention tag, and then select **OK** once the tag is successfully saved.
11. On the menu bar on the top of the page, select the **retention policies** tab.
12. In the **retention policies page**, note that there is one default retention policy. Since this policy is selected by default, its corresponding properties are displayed in the detail pane on the right-side of the screen. This information displays all the default retention tags that have been assigned to this policy.

    You want to create a custom retention policy, so select the **plus (+) sign** icon in the toolbar that appears across the list of existing retention policies.
13. In **new retention policy** window, enter **Office Retention Policy** in the **Name** field.
14. You now want to assign one or more retention tags to this new policy. Below **Retention tags**, select the **plus (+) sign** icon.
15. In the **select retention tags** window, select the **3 Years Move** tag that you just created, select the **add ->** button, and then select **OK**.
16. In addition to the personal retention tag that you just added to the retention policy, you also want to add the following default tags as well:
    - Default 2 year move to archive
    - Deleted Items
    - Junk Email
    - Recoverable Items 14 days move to archive

    Repeat the prior two steps to add these tags to this policy. **Hint:** Hold down the **Ctrl** key as you select each tag in the list; this will enable you to select all four default tags at one time before selecting the **add->** button.

17. On the **new retention policy** window, select **Save** and then select **OK**.
18. You are now going to apply this retention policy to the mailboxes for your two test users, Joni Sherman and Lynne Robbins. In the **Exchange Admin Center**, in the left-hand navigation pane, select **recipients**. In the **recipients** page, the **mailboxes** tab is displayed by default.
19. In the list of recipient mailboxes, select **Joni Sherman** and then select the **pencil (edit) icon** in the toolbar to edit the properties of Joni's mailbox.
20. In the **Edit User Mailbox** for Joni Sherman, select **mailbox features** in the left-hand navigation pane.
21. If a **Warning** dialog box appears, select **OK**.
22. Select the drop-down arrow in the **Retention policy** field and select **Office Retention Policy**.
23. Select **Save** and then select **OK**.
24. Repeat steps 19-23 for **Lynne Robbins**.
25. Leave your web browser open and proceed to the next task.

You have created a new retention policy through the Exchange Admin Center. You assigned several retention tags to this policy, including a custom retention tag, and you assigned the retention policy to Lynne and Joni's mailboxes.

29.0.3 Task 3 – Create a Retention Policy in the Compliance Center

Now that Holly has created a retention policy through the Exchange Admin Center, she wants to do the same in the Compliance Center. For this policy, Holly wants to preserve the content of all Exchange Online mailboxes from deletion for 7 years after the last modification.

1. In **Microsoft Edge**, select the **Office 365 Compliance** center tab if it's still open; otherwise, in the **Microsoft 365 admin center**, under **Admin centers**, select **Compliance**.
2. In the **Office 365 Compliance** center, in the left-hand navigation pane, select **Information governance** and then select **Retention**.
3. In the **Retention** window, select the **+ New Retention Policy** button to start the wizard that's used to create a new retention policy.
4. On the **Name your retention policy** page, enter **Exchange preservation** in the **Name** field and select **Next**.
5. In the **Choose locations to apply the policy** page, as you scroll down the page, note that the **Status** of the **Exchange email** location is turned **On**. Leave this set to On. However, for all the other locations that are turned on, select their toggle switches to turn them **Off**.
6. As you scroll through the locations, **Exchange email** should be the only location turned on.
7. Select **Next**.
8. On the **Decide if you want to retain content, delete it, or both** page, leave the **Retain items for a specific period** option selected, as well as the **7 years**. Do not change these fields.

   However, in the **Start the retention period based on** field, it currently indicates **when items were created**. Select the drop-down arrow for this field and select **when items were last modified**.

   In the **At the end of the retention period** option, select **Delete items automatically**.
9. Select **Next**.
10. On the **Review and finish** page, review all the settings. If any need to be corrected, select the **Edit** option and make the appropriate correction. Once everything looks correct, select **Submit** to finish the wizard.
11. Select **Done**.
12. Do not close your Client 1 VM or Microsoft Edge. Leave your web browser open as well as all tabs for the next lab.

You have now created a new retention policy in the Compliance Center that retains all Exchange emails from all mailboxes for 7 years after the last modification.

30 End of Lab 5

31 Module 6 - Lab 6 - Exercise 1 - Manage DLP Policies

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, your next steps are to implement Data Loss Prevention (DLP) policies at Adatum. You will begin by creating a custom DLP policy in this exercise, and then you'll test DLP policies related to email message archiving and emails with sensitive data.

31.0.1 Task 1 – Create a DLP policy with custom settings

In this lesson you will create a Data Loss Prevention policy in the Security & Compliance Center to protect sensitive data from being shared by users. The DLP Policy that you create will inform your users if they want to share content that contains IP addresses.

The policy will contain two actions, each of which is dependent on the number of IP addresses in the message. If the message contains one IP address, the policy will notify people with a policy tip and still email the message. However, if the content contains at least 2 IP addresses, then the message will be blocked, an incident email with a high sensitivity level will be sent to the sender, and a policy tip will be displayed that allow the sender to override the email blockage if the sender provides a business justification within the policy tip.

IMPORTANT: Unfortunately, you will be unable to test the policy tips in this DLP Policy. When you use the Security and Compliance Center to create a DLP policy that contains a policy tip, the policy tip will NOT be displayed if you also created mail flow rules in the Exchange admin center. If you will recall, back in Module 4, Lab 4, Exercise 1, you created two mail flow transport rules in Exchange, one using the Exchange admin center and the other using PowerShell.

Because you created mail transport rules in the Exchange admin center in the prior lab, policy tips that you configure for DLP policies in the Security and Compliance Center will NOT work. The DLP policy will work, but the policy tip action will not. Even if you delete the mail transport rules, the policy tips will still not function.

Given that, you will still configure a policy tip for the DLP policy that you create in this task; doing so will provide you with experience in configuring policy tips even though you won't be able to verify them. The reason for this is that we also wanted you to experience creating mail transport rules in the earlier lab, even though we knew it meant you would not be able to see the policy tips in this DLP lab.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In **Microsoft Edge**, the Office 365 Security & Compliance Center tab should still be open; if not, then open a new tab and navigate to **https://protection.office.com**.
3. In the **Office 365 Security & Compliance** center, in the left-hand navigation pane, select **Data loss prevention** and then select **Policy**.
4. In the **Policy** window, select **+Create a policy** to start the wizard for creating a new data loss prevention policy.
5. On the **Start with a template or create a custom policy** page, there are four types of policies listed in the left-hand pane - Financial, Medical and health, Privacy, and Custom. The first three (Financial, Medical and health, and Privacy) provide templates that can be used to create a policy. The **Custom** type is not based on a template. The column in the left-hand pane displays the policy type, while the middle pane displays the available templates to choose from for that policy type. When you select a template in the middle pane, the right-hand pane displays the type of information that is protected in that template.

   For example, select **Financial** in the left-hand pane and then scroll through the various templates that you can choose from in the middle pane. Select one or two of the templates to see what type of information it protects. Do the same for the **Medical and health** and **Privacy** policy types.

   Select **Custom** in the left-hand pane, which automatically selects **Custom policy** in the middle pane (since there are no templates to choose from for this policy type). Select **Next**.
6. In the **Name your policy** page, enter **IP Address DLP Policy** in the **Name** field and **Protect IP addresses from being shared** in the **Description** field. Select **Next**.

7. On the **Choose locations** page, select the **Protect content in Exchange email, Teams chats, and channel messages and OneDrive and SharePoint documents** option (if it isn't already selected by default) and then select **Next**.
8. On the **Customize the type of content you want to protect** page, select the **Find content that contains:** option (if it isn't already selected by default).
9. Under **You must select at least one classification type**, select **Edit.**
10. In the **Choose the types of content to protect** page, select the **Add** drop-down field, and in the drop-down menu, select **Sensitive info types**.
11. In the **Sensitive info types** window, select **(+) Add**.
12. In the search field type **Address** and wait until the search results are displayed.
13. In the list of search results, select the **IP Address** check box and then select **Add.**
14. Once you receive the message indicating **1 sensitive info type added,** select **Done**.
15. On the **Choose the types of content to protect** window, under the **Content contains** bar, select **Any of these** in the drop-down field (this should be selected by default), and then select **Save**.
16. On the **Customize the type of content you want to protect** page, **IP Address** should now appear under the **Find content that contains** option.
17. Verify that the **Detect when this content is shared:** check box is selected.
18. In the field below this, select the drop-down arrow and select **only with people inside my organization**.
19. Select **Next**.
20. On the **What do you want to do if we detect sensitive info?** page, there are two groups of settings that you must configure:
    - Under the **Notify users when content matches the policy settings** section, verify the **Show policy tips to users and send them an email notification** check box is selected. Select **Customize the tip and email**.

      In the **Customize policy tips and email notifications** window, the email notification option to **Notify the user who sent, shared, or last modified the content** option is selected by default; leave this as is.

      However, sending policy tips is not selected by default, so select the **Customize the policy tip text** check box (otherwise, a policy tip will not be displayed). In the policy tip field that appears, enter **Warning: The email contains sensitive info (IP Address).** Select **OK**.
    - Under the **Detect when a specific amount of sensitive info is being shared at one time** section, verify the **Detect when content that's being shared contains** option is selected. In the field below this, **10** is entered. Change this to **2** and then select **Next.**
21. On the **Customize access and override permissions** page, the **Let people who see the tip override the policy** option is turned On by default. Leave this option **On**, but also select the **Require a business justification to override** check box, and then select **Next**.
22. On the **Do you want to turn on the policy or test things out first?** page, select **Yes, turn it on right away** and then select **Next**.
23. Check the configuration on the **Review your settings** page. Two actions should be displayed (these are dependent on the number of IP addresses in the message):
    - If the content contains an IP address, then notify people with a policy tip and email the message.
    - If there are at least 2 instances IP addresses, then block access to the content and send an incident report with a high sensitivity level but allow people to override it if they provide a business justification.

    Select **Back** if you need to correct any settings, and then select **Create** once you're satisfied with the settings.

You have now created a DLP policy that scans for IP addresses in emails and documents that are sent or shared in your organization.

32 Proceed to Lab 6 - Exercise 2

33 Module 6 - Lab 6 - Exercise 2 - Test MRM and DLP Policies

You are now at the point in your pilot project where you want to test the MRM and DLP policies that you created in previous lab exercises. You have decided to test the MRM policy that affects how email messages are archived, and then you want to test the DLP policy related to emails that contain sensitive information.

33.0.1 Task 1 – Test an MRM Policy to Archive Email Messages

In this exercise, you will send an email from Holly Dickson to one of your pilot team users, Lynne Robbins. You will then log into Microsoft 365 as Lynne on the LON-CL2 VM, locate the email in her Inbox, and then assign the email a custom retention tag that you created. This personal retention tag will override the parent folder tag for this specific message, which will be moved to Lynne's In-Place archive mailbox after 3 years rather than 2 years.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In **Microsoft Edge**, select the **Microsoft Office Home** tab, and then select the **Outlook** icon in the column of app icons on the left-side of the screen. When Outlook on the web opens, you should be automatically logged in as Holly Dickson.

   Note: If **Outlook on the web** was already open, then verify that you are logged in as **Holly** by checking the user icon in the upper right corner (the **HD** circle). If Outlook was open for any other user, then close the tab and repeat the instructions in this step to open Outlook on the Web for Holly.
3. In **Outlook on the web**, in the upper left corner of the screen, select **+New message**.
4. In the message pane that appears, enter the following information:
   - To: enter **Lynne** and then select **Lynne Robbins** from the user list that appears
   - Add a subject: **Archive Test**
   - Message area: type **Use this email to test archiving.**
5. Select **Send**.
6. Switch to LON-CL2.
7. If necessary, log in as the **Admin** with a password of **Pa55w.rd**.
8. In the **Edge** browser, you should have one tab open with Outlook on the web for Alex Wilber. Select Alex's user icon in the upper right-hand corner of the screen, and in the **My account** window that appears, select **Sign out**.
9. In the browser tab in which you are signed out, enter the following URL in the address bar: **https://outlook.office365.com**
10. You want to sign into **Outlook on the web** as **Lynne Robbins.** In the **Pick an account** window, select Lynne Robbins' user account (**LynnR@xxxxxZZZZZZ.onmicrosoft.com**).
11. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
12. In **Outlook on the web**, in Lynne's **Inbox**, you should see the email message that Holly just sent to Lynne.
13. Back in Lab 3, you changed the assigned retention policy for Lynne's mailbox to **Office Retention Policy**. This policy contains the **3 Year Move – Archive after three years** personal retention tag that you created in Lab 3.

    Upon receiving this email from Holly, Lynne has decided to tag Holly's email to automatically archive it after three years instead of two years, which is the default policy.

    To accomplish this, begin by selecting the **Settings** icon in the upper right corner of the toolbar (the gear-shaped icon).
14. In the **Settings** pane that appears, select **View all Outlook settings**.

15. In the **Settings** window that appears, the **Mail** option is already selected by default in the left-hand pane. In the middle pane, select **Retention policies**.
16. In the **Retention policies** pane that appears on the right side of the screen, select **+Add new policy**.
17. In the **Retention policies** pane, after a few seconds the default and custom retention policies will appear. Scroll to the bottom and select the **3 Year Move - Archive after three years** retention policy that you created in a prior lab, and then select **Save**.
18. Verify you selected the correct retention policy and then close the **Settings** window by selecting the **X** in the upper right corner. This returns you to Lynne's mailbox.
19. In the **Inbox**, right-click the message that she received from Holly with the subject: **Archive Test**. In the menu that appears, scroll to the bottom and select **Advanced actions**, and then in the menu that appears, select **Assign policy**. In the **Assign Policy** menu that appears, under the **Archive Policy** section, select **3 Year Move - Archive after three years.**

    Note: This personal retention policy will now override the parent folder policy for this specific message, which will be moved to Lynne's In-Place archive mailbox after 3 years.
20. Leave Outlook on the web open in the LON-CL2 VM as you will return there as Lynne in the next task after receiving another email from Holly.

33.0.2 Task 2 – Test a DLP Policy for Sensitive Emails

In the previous exercise, you created a custom DLP policy that searches emails for sensitive information related to IP addresses in your Adatum tenant. In this exercise, you will send two emails from Holly Dickson to Lynne Robbins; the first will include one IP address, and the second email will include two IP addresses. You will verify how each email is handled as a result of the DLP policy.

If you will recall, in the DLP policy that you created, if one IP address is discovered in an email, an email policy tip is displayed in sender's Outlook mailbox that informs the sender the email contained sensitive data. The sender will also receive an email notification, and the email with the sensitive data (in this case, the IP address) will still be sent to the recipient.

However, the email will be blocked if two or more IP addresses are discovered in the mail. An email policy tip is displayed in Outlook for the sender just as before, but in this case, the DLP policy was set up to allow the sender to override the blocked email and allow it to be sent.

Important: Unfortunately, you will be unable to test the policy tips in this task. As was mentioned in the prior exercise, when you use the Security and Compliance Center to create a DLP policy that contains a policy tip, the policy tip will NOT be displayed if you also created mail flow rules in the Exchange admin center. If you will recall, back in Module 4, Lab 4, Exercise 1, you created a mail flow transport rule in the Exchange admin center. As a result, the policy tips that you configured for DLP policies in the Security and Compliance Center will NOT work. The DLP policy will work, but the policy tip will not be displayed. Even if you delete the mail transport rules, the policy tips will still not function.

Therefore, when you send an email with two IP addresses in this task, all you can do is verify that the email message is blocked. The policy tip will not display; therefore, you will be unable to override the blockage and send the email. While we wanted you to experience creating mail transport rules in the earlier lab, we also knew this would not allow you to see policy tips in this lab. But it was felt that learning how to create mail transport rules in the earlier lab was worth this minor inconvenience in this lab.

1. Switch to LON-CL1, where you should still be logged into Microsoft 365 as Holly Dickson.
2. You will now send an email from Holly to Lynne, and you will include an IP address in the body of the email. In **Microsoft Edge**, the **Outlook on the web** tab should still be open for Holly. If necessary, select the **Outlook on the web** tab.
3. In the upper left corner of the screen, select **+New message**.
4. In the message pane that appears on the right-side of the screen, enter the following information:
    - To: enter **Lynne** and then select **Lynne Robbins** from the user list that appears
    - Add a subject: **DLP Policy Test**
    - Message area: type **I will configure this IP address: 192.168.0.1.**

Note: When drafting this email with sensitive data (in this case, an IP address) that triggers the DLP policy, a policy tip should be displayed indicating the email violated a DLP policy. Unfortunately, the policy tip will not be displayed as previously mentioned.

5. Select **Send.**
6. Holly should receive an email in her Inbox from **Microsoft Outlook** with the subject **Notification:** (in this case, should be the name of the policy you created that tested for IP addresses in emails, which was **DLP policy test**). Review the content of this email.
7. You will now send a second message from Holly to Lynne that contains multiple IP addresses. Repeat the process as before for creating an email to Lynne Robbins with the following information:
   - Add a subject: **Second DLP Policy Test**
   - Message area: **Test IP address 192.168.0.1 and then IP address 172.16.0.1.**

   Note: When drafting this email with sensitive data (in this case, two IP addresses) that triggers the DLP policy, a policy tip should be displayed indicating the email violated a DLP policy. Because there are two IP addresses, the policy tip would indicate that the email will be blocked, but it would give you the option to override the blockage by entering a business justification for sending this sensitive data. Unfortunately, the policy tip will not be displayed as previously mentioned.
8. Immediately after sending the email, Holly should receive two emails in her Inbox from **Microsoft Outlook**.
   - The first email should have the subject **Rule detected - High volume of content detected IP address DLP policy**. Select this email and review its contents.
   - The second email should be a **Message Blocked** notification for the email that you just sent. Select this email to review its contents.
9. Switch to LON-CL2.
10. If you need to sign into the VM, the **Admin** account should appear by default, so enter **Pa55w.rd** in the **Password** field to log in.
11. You should still be logged into **Outlook on the Web** in the LON-CL2 VM as **Lynne Robbins**. In your **Edge** browser, Lynne's mailbox should still be open in **Outlook on the web** from when you last used it in the previous task.
12. In Lynne's **Inbox**, you should see the first message (**DLP policy test**) that you sent, but not the second (**Second DLP policy test**). Remember, when Holly sent the second email, she received a notification that it had been blocked.
13. Leave your Edge browser and all its tabs open on LON-CL2.

34 End of Lab 6

35 Module 7 - Lab 7 - Exercise 1 - Implement Sensitivity labels with Azure Information Protection Unified Labels client

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, your next steps are to implement Sensitivity Labels with Azure Information Protection (AIP) and Windows Information Protection (WIP) at Adatum.

IMPORTANT: This lab exercise consists of four tasks. In the first task you will install the AIP Unified Labeling Client, and in the second task you will create a sensitivity label and assign it to the default sensitivity label policy. The final two tasks validate the sensitivity label and label policy. The problem with this lab is that when you create a sensitivity label and label policy, it takes up to 24 hours for the label and label policy to propagate through the system. **This means that you can perform the first two tasks, but then you must wait until the next day before you can perform the final two tasks.**

35.0.1 Task 1 – Install the Azure Information Protection Unified Labeling client

To implement Sensitivity labels as part of your pilot project at Adatum, you must first install the AIP client from the Microsoft Download Center.

1. At the end of the prior lab, you were on LON-CL2. Switch to **LON-CL1**.

   You should still be logged into LON-CL1 as the **admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.

2. In **Microsoft Edge**, open a new tab and enter (or copy and paste) the following URL in the address bar: **https://www.microsoft.com/en-us/download/confirmation.aspx?id=53018**

   This will start the download for the AIP Unified label client.

3. In the Microsoft download center tab, a notification bar will appear at the bottom of the page asking whether you want to Run, Save, or Cancel. Select **Run**. If you do not receive this notification, select **Open file** in the download bar at the bottom left.

4. The Microsoft Azure Information Protection wizard will open. If the wizard does not display on the desktop, select the icon for the wizard on the taskbar to display the wizard.

5. In the wizard, on the **Install the Azure Information Protection client** page, clear (uncheck) the **Help improve Azure Information Protection by send usage statistics to Microsoft** check box and then select the **I agree** button.

6. If a **User Account Control notification** dialog box appears that asks whether the app is allowed to make changes to this device, select **Yes**.

7. Once the installation is complete, select **Close**.

8. In your Edge browser, close the **Download** tab that you opened in this task to download the Azure Information Protection client.

You have successfully installed the AIP Unified Label client on Client 1 VM.

35.0.2 Task 2 – Create a Sensitivity Label

In this exercise you will create an Sensitivity Label and add it to the default policy so that it's valid for all users of the Adatum tenant.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.

2. In **Microsoft Edge**, select the **Data loss prevention** tab that displays the **Office 365 Security & Compliance** center.

3. In the **Office 365 Security & Compliance** center, in the left-hand navigation pane, select **Classification**, and then select **Sensitivity labels.**

4. In the **Home > sensitivity** window, three tabs are displayed across the top of the page. The **Labels** tab is displayed by default.

   On the **Labels** tab, a warning message is displayed in the middle of the screen indicating **Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint.**

   Select the **Turn on now** button that appears on the right side of this message. This will enable Adatum to apply the Sensitivity labels inside its Microsoft 365 environment.

5. On the **Labels** tab, select **+Create a label** that appears in the middle of the screen on the menu bar. This initiates the **New sensitivity label** wizard.

6. In the **New sensitivity label** wizard, on the **Name and create a tooltip for your label** page, enter the following information:

   - Name: **PII**
   - Display name: **PII**
   - Description for users: **Documents, files, and emails with PII**
   - Description for admins: **Documents, files, and emails with PII**

7. Select **Next**.
8. On the **Define the scope for this label** page, confirm that the **Files & Emails** check box is selected and then select **Next**.
9. On the **Choose protection settings for files and emails** page, select both check boxes for **Encrypt files and emails** and **Mark the content of files**, then select **Next**.
10. On the **Encryption** page, select the **Remove encryption if the file is encrypted** option and then select **Next**.
11. On the **Content Marking** page, set the **Content Marking** toggle switch to **On** and then select all three check boxes. Under each setting, select **Customize text** and then enter the following information for each option (select **Save** after entering the settings for each option):
    - Add a watermark
        - Watermark text: **Sensitive - Do Not Share** (Hint: after entering this value, copy it so that you can paste it in the other two text settings)
        - Font size: **25**
        - Font color: **Blue**
        - Text layout: **Diagonal**
    - Add a header
        - Header text: **Sensitive - Do Not Share**
        - font size: **25**
        - Font color: **Red**
        - Align text: **Center**
    - Add a footer
        - Footer text: **Sensitive - Do Not Share**
        - font size: **25**
        - Font color: **Red**
        - Align text: **Center**
12. On the **Content Marking** page, select **Next**.
13. On the **Auto-labeling for Office apps** page, set the **Auto-labeling for Office apps** toggle switch to **On**. This enables a series of options that you will update in the next steps.
14. Under **Detect content that matches these conditions**, select **+Add condition** and then select **Content contains**.
15. In the **Content contains** window, select the **Add** drop-down arrow and then select **Sensitive info types**.
16. In the **Sensitive info types** window, select the **Select all** check box and then select **Add**.
17. All of the sensitive information types will be displayed. Scroll to the bottom on the window and update the following settings:
    - When Content Matches these conditions: select **Automatically apply the Label**
    - Display this message to users when the label is applied: enter **Sensitive content has been detected and will be encrypted**.
18. Select **Next**.
19. On the **Define protection settings for groups and sites** page, do not select either check box. Select **Next**.
20. On the **Auto-labeling for database columns** page, do not enable Auto-labeling for database columns. Select **Next**.
21. On the **Review your settings and finish** page, review the information you entered. If any settings need to be corrected, select the corresponding **Edit** option. When all information appears correct, select **Create label**.
22. An **Error** dialog box should appear that states the generated rule blob for the label you are attempting to create is too long. The maximum size of sensitive information type selections you can make at one

time per rule is **49152**. By selecting all the sensitive information types like you did in the **Sensitive info types** window a few steps back, you have exceeded this limit. **We purposely had you select all the sensitive information types so that you would receive this error.** We wanted you to experience this error so that if it happens in your production environments, you will know why you received the error and how you can correct it.

To correct this issue, select **OK** in the **Error** dialog box, and then on the **Review your settings and finish** page, scroll down to the **Auto-labeling for Office apps** section and select **Edit**.

23. On the **Choose protection settings for files and emails** section of the wizard, select **Next** on the **Encryption** page, and then select **Next** on the **Content Marking** page. This will take you to the **Auto-labeling for Office apps** page.
24. On the **Auto-labeling for Office apps** page, to the right of the **Content contains** condition, select the **trash can icon**. This will remove the existing **Content contains** condition for the **PII** label.

    In the remaining steps, you will add a new condition that only contains two sensitivity information types rather than all the sensitivity information types like you did originally.
25. On the **Auto-labeling for Office apps** page, under **Detect content that matches these conditions**, select **+Add condition** and then select **Content contains**.
26. In the **Content contains** window, select the **Add** drop-down arrow and then select **Sensitive info types**.
27. In the **Sensitive info types** window, in the list of sensitive information types, this time only select the **ABA routing number** and the **U.S. Social security Number (SSN)** check boxes, select **Add**, and then select **Next**.
28. On the **Define protection settings for groups and sites** page, select **Next**.
29. On the **Auto-labeling for database columns** page, do not enable Auto-labeling for database columns. Select **Next**.
30. On the **Review your settings and finish** page, select **Create label**.
31. On the **Your label was created** page, select **Done**.
32. Now its time to publish the **PII** label. On the **Labels** tab, the **PII** label that you just created is the only label in the list. Select **PII** label.
33. In the **PII** window that appears, select the **Publish label** button. This initiates a **Create policy** wizard.
34. In the **Create policy** wizard, on the **Choose sensitivity labels to publish** page, the **PII** label is already listed, so select **Next**.
35. On the **Publish to users and groups** page, select **Choose users or groups**.
36. On the **Edit Locations** page, select **+Add**. A new window will appear that displays all the Adatum users and groups. Select the top check box to the left of the **Name** field, which will automatically select all the check boxes. Select **Add** and then select **Done**.
37. On the **Publish to users and groups** page, select **Next**.
38. On the **Policy settings** page, select the **Apply this label by default to documents and emails** field, and in the drop-down menu that appears, select **PII**. Select the **Users must provide justification to remove a label or lower classification label** checkbox, and then select **Next**.
39. On the **Name your policy** page, enter **PII Policy** in the **Name** field, and then enter (or copy and paste) the following description for this sensitivity label policy: **The purpose of this policy is to detect sensitive information such as ABA bank routing numbers and US social security numbers in emails and documents, and to encrypt this information when it's discovered. The user must provide an explanation for removing the classification label.** Select **Next**.
40. On the **Review and finish** page, review the information you entered. If anything needs to be corrected, select the corresponding **Edit** option and make the corrections. When all information is correct, select **Submit**.
41. On the **New policy created** page, select **Done**.

STOP!! As mentioned at the start of this lab exercise, now that you have created a sensitivity label and assigned it to the default policy, you must wait 24 hours for the label and label policy to propagate through the system before you can perform the next two tasks in this exercise.

Do NOT proceed to the next task! You can continue with the training course and perform the next series of lab exercises. However, when you reach a good break time tomorrow, you should return to this lab exercise and continue with Task 3. When you get to step 14, if you do NOT see the **Sensitiviy** group in the Word ribbon, then you must wait until such time that it appears. **The appearance of the Sensitivity group in the Word ribbon is the indicator as to whether the sensitivity label has completed its behind-the-scenes provisioning,** at which time you can complete tasks 3 and 4 of this lab exercise.

35.0.3 Task 3 – Assign your Sensitivity Label to a document

In this exercise you will use the Sensitivity label that you created in the previous task to classify a document. For this task, you will sign into Microsoft 365 as Alex Wilber, who is a regular user without any elevated privileges.

IMPORTANT: You should not perform this task until you have waited 24 since you completed the prior task. After creating the sensitivity label and label policy in task 2, it takes 24 hours for the label and label policy to propagate through the Microsoft 365 system.

You will know when the propagation is complete and that you can continue with this task when you get to step 14 and you see the Sensitivity label group in the Word ribbon. If this group does not appear, then the label provisioning process has not finished. If this occurs, then wait until your next break time in class and check this again.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. To validate the sensitivity label that you created in the prior task, you must first sign out of Microsoft 365 as Holly and sign back in as Alex Wilber.

   In your Edge browser, select the **Microsoft 365 admin center** tab, and then select the circle with Holly Dickson's HD initials in the upper right corner of the screen. In the **Holly Dickson** window, select **Sign out**.
3. Once you are signed out, close all the tabs in your Edge browser except for the **Sign out** tab.
4. In the **Sign out** tab, enter the following URL in the address bar: **https://portal.office.com/**
5. In the **Pick an account** window, select **Use another account**.
6. In the **Sign in** window, enter **AlexW@xxxxxZZZZZZ.onmicrosoft** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**.
7. On the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
8. If a **Get your work done with Office 365** window appears, select the X to close it.
9. On the **Microsoft Office Home** tab, select the **Word** icon in the column of app icons on the left-side of the screen. This will override the **Microsoft Office Home** tab by opening Microsoft Word Online in this same tab.

   Note: In the next task, you will return back to the **Microsoft Office Home** tab by selecting the **Back** arrow at the top of this **Word** tab.
10. In the **Word** tab, select **New blank document**.
11. If a **Your privacy option** window appears, select **Close**.
12. If the Word ribbon displays icons for each feature but does not break the icons out by group, then select the down-arrow on the far right-side of the ribbon. This will switch the ribbon to the traditional ribbon style that is broken out by feature group (such as Undo, Clipboard, Font, Paragraph, Styles, and so forth).
13. In the **Word** document, type **Testing personally identifiable information (PII).**
14. Because you enabled Sensitivity labels at the start of this exercise, and assuming it's been 24 hours since you created the sensitivity label in the prior task, Word should display a **Sensitivity** group on the ribbon.

    IMPORTANT: If you do not see this **Sensitivity** group in the ribbon, then Microsoft 365 has not finished provisioning the sensitivity label that you created in the prior task. If this occurs, then you

cannot proceed with this task. As mentioned earlier, it takes 24 hours for a new sensitivity label to be fully provisioned throughout the system. If you do not see the Sensitivity group, or if you see the group (from a prior label you created) and you select the drop-down arrow in the group and do not see your new label, then you must stop at this point and not proceed until you see the Sensitiity group and your label in the group.

Assuming you have waited 24 hours and the **Sensitivity** group appears in the Word ribbon, select the down arrow in the **Sensitivity** group. In the drop-down menu that appears, it should display the **PII** label that you created in the prior task. Since the **PII** label is enabled for this document, a check mark is displayed next to **PII**.

In this first validation test, you are going to attempt to remove this sensitivity label from being applied to this document. If you'll recall, when you created the label policy and assigned the PII label to it, you selected the option whereby users must provide justification to remove a label or to select a lower classification label. You will now verify whether this setting is functioning properly.

To remove the label from this document, select the **PII** label that appears in this drop-down menu.

15. In the **Justification Required** window that appears, select the **Other (explain)** option. In the **Explain why you're changing this label** field, enter **Testing what happens when a label is removed** and then select **Change**.
16. In the **Sensitivity** group in the Word ribbon, select the down arrow. In the drop-down menu that appears, note that while **PII** is displayed, it no longer has a check mark displayed next to it. This indicates the PII sensitivity label is no longer being applied to this document.
17. To re-apply the sensitivity label to the document, select **PII** in the drop-down menu. Once again select the drop-down arrow in the **Sensitivity** group. The drop-down menu that appears should display the **PII** label, and it should display a check mark next to it that indicates it is being applied to this document.
18. In the Word document, enter **111-11-1111** below the previous line of text that you entered. This number is the same format as a U.S. Social Security Number.
19. You will now save the document. On the title bar, to the right of Word, select **Document1**. In the drop-down menu that appears, confirm the file **Location** says **Alex Wilber>Documents**.

    In the **File Name** field, rename the file to **ProtectedDocument1** and then select outside of this file name menu (select inside the document). Note the new name assigned to the file in the title bar.
20. On the right-side of the menu bar, select the **Share** button.
21. In the **Send link** window that appears, select **Anyone with the link can edit**. In the menu that appears, select **Specific people** then select **Apply**.
22. In the **Send link** window, enter **Joni** in the **Enter a name or Email address** field. In the list of users that appears, select **Joni Sherman** and then select **Send**.
23. Close the **Link sent** window.

You have just successfully created an AIP protected Word document that is read-only protected. The document is accessible only by its creator, Alex Wilber, and by Joni Sherman (with Read-only permission), to whom the document was shared.

35.0.4 Task 4 – Verify your Sensitivity Label policy

In the prior task, you created a Word document and protected it with a Sensitivity label. The PII label policy should have inserted a watermark in the document, and it should have restricted permissions on the document. To verify whether the protection that you assigned to the document works, you will first email the document to Joni Sherman and to your own personal email address. You will then test what functionality is possible for both Joni and Alex Wilber.

1. You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Alex Wilber**.
2. In your Edge browser, select the **Word** tab and then select the **Back** arrow. This should display the **Microsoft Office Home** tab.
3. In the **Microsoft Office Home** tab, select the **Outlook** icon in the column of app icons on the left-side of the screen. This opens Outlook on the web in a new tab.

4. In **Outlook on the web**, select **New Message** in the upper left part of the screen.
5. In the right-hand pane, enter the following information in the message form:
   - To: Enter **Joni** and then select **Joni Sherman** from the user list.
   - CC: Enter your own personal email address (do NOT enter Holly's email address; instead, enter your own personal email address)
   - Add a subject: **Protected Document Test**
   - Body of the message: enter **If you can open the protected and restricted document attached to this email, then try to change it.**
6. Select **Attach** from the menu bar at the top of the screen, and in the drop-down menu that appears, under the **Suggested attachments** group, select the **ProtectedDocument1.docx** file that you created in the prior task.
7. Once the file has been attached to the email, select the file to open it. Note the watermarks that appear in the header and footer, and in the body of the document. After reviewing the document, select the **X** in the upper right corner of the document window to close it.
8. Select **Send**.
9. Switch to LON-CL2.
10. In LON-CL2, you should be logged into **Outlook on the Web** as **Lynne Robbins** from a previous lab exercise. Sign out as Lynne.
11. In your Edge browser, in the **Sign out** tab, enter the following URL in the address bar: **https://outlook.office365.com**
12. In the **Pick an account** window, select **Use another account**.
13. In the **Sign in** window, enter **JoniS@xxxxxZZZZZZ.onmicrosoft** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**.
14. On the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.
15. If a **Welcome** window appears, select the X to close it.
16. In Joni's **Inbox** in **Outlook on the web**, open the email that Alex just sent her by selecting the email in the Inbox. Note the **Sensitive - Do Not Share** watermark that appears in the message (these are the header and footer watermarks that you entered in the PII label).
17. Select the attached file to open it.
18. In the **Your privacy option** dialog box that appears, select **Close**. Review the document, and note the watermarks in the header, footer, and body of the document. Close the document window.
19. This will return you to **Outlook on the web** with the email still displayed in the right-hand pane. In the body of the email, the document appears in a tile. You want to download the document. Hover your mouse over the document tile and note the two down arrows that appear. Hover your mouse over each arrow. The first displays **Download**, while the second arrow displays **More actions**. Select the **More actions** arrow, and in the drop-down menu that appears, note that it also has a **Download** option. Since you have this menu open, select the **Download** option from here.
20. In the notification bar that appears at the bottom of the screen, select **Save.**
21. Once the file has finished downloading, in the notification bar, select **Open.**
22. **Microsoft Word** should open along with a **Sign in** window (it may open behind the Outlook window, in which case select the **Word** icon on the taskbar to bring it forward).
23. Because the file is RMS protected and no AIP unified labeling client is installed on LON-CL2, you need to use the native RMS features of Word Microsoft Apps and register this installation to Joni's account.

    In the **Sign in** window, enter **JoniS@xxxxxZZZZZZ.onmicrosoft.com** and then select **Next.**
24. In the **Enter password** window, enter **Pa55w.rd** and then select **Sign in.**
25. In the **Use this account everywhere on your device** window that appears, select **This app only** to register this Office 365 ProPlus installation to **Joni Sherman's** Microsoft 365 account.

26. The file should open in Word, since you assigned Joni with Read-only permission. Review the three notification bars that appear above the document.

27. Try to change the file. Word should not recognize any keystrokes, and it should display the following message above the taskbar: **This modification is not allowed because the document is open for viewing only.**

    Note: You have just verified that the permissions assigned to the file are working properly. Joni can read the file (since she was assigned Read-only permission), but she is unable to change it (no one was assigned Edit permission).

28. Close Word.

29. You will now test what happens when you attempt to open the document that was sent to your personal email address. Use your phone or classroom PC to access your personal email address. Open the email that you (in the role of Holly) just sent to your personal email address, and then attempt to open the attached file.

30. You should receive a messaging indicating that you are not signed into Office with an account that has permission to access the document. You can optionally sign in with an account that has permission to access the file, or request access from the **AlexW@xxxxxZZZZZZ.onmicrosoft.com** account, or Cancel out of the operation. Select **Cancel**.

    Since only Joni was assigned permission to read the document, you just verified that Azure Information Protection protected the document based on the PII policy parameters that you configured.

31. Remain signed into LON-CL2 and signed into Outlook on the Web as Joni. Do not close your browser.

36 Proceed to Lab 7 - Exercise 2

37 Module 7 - Lab 7 - Exercise 2 - Implement Windows Information Protection

Now that Holly Dickson has implemented Sensitivity labels as part of her pilot project at Adatum, she is ready to implement Windows Information Protection (WIP). In your role as Holly Dickson, you will use this exercise to create a WIP policy that will be applied to any member of the WIP Users group who has an MDM-enrolled device in Intune.

37.0.1 Task 1 – Configure Windows Information Protection

In this lesson you will create a WIP policy and assign to it the **WIP Users** group that you created in an earlier lab. This policy will protect files in Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus) for users in the **WIP Users** group that have enrolled Windows 10 devices. You will perform this task on LON-CL1, so you must begin by signing out of Microsoft 365 as Alex Wilber and signing back in as Holly Dickson.

1. At the end of the prior lab exercise, you were using LON-CL2. Switch to **LON-CL1**.

   You should still be logged into LON-CL1 as the **Admin** account, and you should be logged into Microsoft 365 as **Alex Wilber.**

2. In the **Edge** browser, select the **Microsoft Office Home** tab and then select Alex's user icon in the upper right-hand corner of the screen. In Alex's account window that appears, select **Sign out**. Close all browser tabs except for the **Sign out** tab.

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

4. In the **Pick an account** window, select **Holly Dickson's** account (Holly@xxxxxZZZZZZ.onmicrosoft.com) if it appears; otherwise, select **Use another account**, and then on the **Sign in** window, enter Holly's' user account (**Holly@xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**.

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

6. In the **Microsoft Office Home** tab, select the **Admin** icon in the column of app icons that appears on the left-side of the screen. This opens the Microsoft 365 admin center.

7. In the **Microsoft 365 admin center**, select **Show all** in the left-hand navigation pane, and then under the **Admin centers** group, select **Endpoint Manager**.
8. In the **Microsoft Endpoint Manager admin center**, in the left-hand navigation pane select **Apps**.
9. In the **Apps | Overview** page, in the middle pane under the **Policy** group, select **App protection policies**.
10. On the **Apps | App protection policies** page, select **+Create Policy** on the menu bar, and then in the drop-down menu that appears, select **Windows 10**.
11. In the **Create policy** window, the steps to create a policy are displayed at the top of the page. You are currently in step **1 - Basics**. Enter the following information and then select **Next**:
    - Name: **WIP Client Protection**
    - Description: leave blank
    - Enrollment state: **With enrollment**
12. In the **Create policy** window, you are now in step **2 - Targeted apps**. Enter the following information and then select **Next**:
    - Protected apps: select **+Add**. In the **Add apps** pane that appears on the right, scroll to the bottom and select **Office-365-ProPlus-1810-Allowed.xml**, and then select **OK**.
    - Exempt apps: leave blank as there will be no exempt apps in this policy
13. In the **Create policy** window, you are now in step **3 - Required settings**. Enter the following information and then select **Next**:
    - Windows Information Protection mode: **Block**
    - Corporate identity: verify that it displays **xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **OK.**
14. In the **Create policy** window, you are now in step **4 - Advanced settings**. Do not change any of the default settings, so select **Next**.
15. In the **Create policy** window, you are now in step **5 - Assignments**. Enter the following information and then select **Next**:
    - Selected groups: select **+Select groups to include**. In the **Select groups to include** pane that appears on the right, select the **WIP Users** group and then select the **Select** button at bottom of the pane.
16. In the **Create policy** window, you are now in step **6 - Review + create**. Review the settings and if anything is incorrect, select the **Previous** button to return back to the appropriate step to make your correction. If all the settings are correct, then select the **Create** button.
17. On the **Apps | App protection policies** window, note the value of the **Deployed** column is **No** for the **WIP Client Protection** policy that you just created. Select **Refresh** on the menu bar above the list of policies. The **Deployed** status should now display **Yes**.
18. Leave your browser and all its tabs open for the next lab.

You have now created an **App protection policy** (which is a Windows Information Protection policy) that protects files in Microsoft 365 Apps for enterprise for users in the **WIP Users** group that have enrolled Windows 10 devices.

37.0.2 Task 2 – Use Windows Information Protection

In this exercise you will enroll your LON-CL2 device to Azure AD. You will then test the WIP policy that you created in the prior task by creating a work document and then copy and pasting from it to a personal location. This will test the WIP protection feature that prevents copy and pasting between a protected Word document and an untrusted website in your Edge browser. Since the WIP policy that you created was assigned to the WIP Users group, you must switch to LON-CL2 and create the document while signed in as Joni Sherman, who is a member of this group.

1. Switch to LON-CL2, where you should still be logged in as the **Admin** account, and you should be logged into **Outlook on the Web** as **Joni Sherman**.

2. Minimize your **Edge** browser.
3. In the **Search** box on the taskbar at the bottom of the window, type **Work** (not **Word**, but **Work**). In the menu that appears, if **Settings** is not expanded, then select it now. Under **Settings**, select **Access work or school**.
4. In the **Access work or school** window, select **Connect**.
5. In the **Set up a work or school account**, enter **JoniS@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **Email address** field and then select **Next**.
6. On the **Enter password** window, enter **Pa55w.rd** and select **Sign in**.
7. If a **More information** is required dialog box appears, select the X in the upper-right corner to close it.
8. In the **Access work or school** window, Joni's email address now appears as a work or school account. Close the **Settings** window.
9. Select the **Start** icon in the the bottom left corner of the taskbar, and in the **Start** menu, select **Microsoft Word**.
10. Select **Blank document**.
11. If a **What's New** window opens, close it.
12. In the document, type **Protected business content**.
13. Select **File** from the menu bar above the ribbon, select **Save As** on the left menu, and then select **Browse** from the **Save As** menu.
14. In the **File Explorer** window, you should see a **lock symbol** that appears to the left of the **File name** field. Next to this lock symbol is a drop-down arrow. Select this arrow, and in the menu that appears, select **Work (xxxxxZZZZZZ.onmicrosoft.com).**
15. Accept the default file name **Protected business content.docx**, change the file path to your **Documents** folder and select **Save**.
16. In the Word document, select the sentence that you typed in the document, then right-click on the selected text and select **Copy**.
17. Select the **Edge** icon on the taskbar. In your browser, open a new tab, click in the Search box and press **Ctrl-V** on your keyboard to paste in the copied text. Instead of seeing the copied text, a pop-up window should appear with the following message: **Can't use work content here. Your organization doesn't allow you to use work content here.** Select **OK**.

    You have just verified that WIP protection prevents copy and pasting between a protected Word document and an untrusted website in your Edge browser.
18. Leave your LON-CL2 VM and browser open for the next lab.

You have just enrolled the Client 2 VM to your tenant, so the Client app protection policy **WIP Client Protection** that you configured in the last task could be applied to protect the content of a Word document.

38 End of Lab 7

39 Module 8 - Lab 8 - Exercise 1 - Implement a Data Subject Request

Data subject requests (DSRs) are used to search for and extract all known information on a person of interest. A DSR can come from the person in question or from an authorized source. In this exercise you will configure and export a DSR from the Office 365 Security and Compliance center.

IMPORTANT: You should only run a DSR if the request is made by a Data Privacy officer or a Human Resources manager. Due to data privacy legal concerns, you should NEVER run a DSR unless instructed to do so.

39.0.1 Task 1 – Create a GDPR Data Subject Request

Holly Dickson is Adatum's Enterprise Administrator. In her role as the company's Microsoft 365 Enterprise Administrator, she is responsible for implementing Adatum's Microsoft 365 pilot project. Since Adatum has several European subsidiaries, properly managing GDPR data subject requests is a key task that must be tested so the company can successfully implement this feature in accordance with EU law. In this task, Holly will create a DSR for herself on behalf of a request made by Adatum's Human Resources department.

Note: To perform this task, Holly must be assigned to the eDiscovery Manager role group so that she has the necessary permissions. You added Holly to this role group in Lab 1 at the same time that you added Joni Sherman to the role group. The reason why you were instructed to add Holly to the eDiscovery Manager role group in Lab 1 rather than at the start of this lab is that it can sometimes take up to an hour or more for permissions to successfully propagate. If you had assigned Holly to this role group just prior to this query, you would have received error messages involving parameter fields because her permissions would not have completed propagating. By adding Holly to this role group at the start of this course, enough time will have elapsed between then and now for the propagation to complete.

1. Switch to LON-CL1, where you should still be logged in as the **Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson** (**holly@xxxxxZZZZZZ.onmicrosoft.com**) with a password of **Pa55w.rd**.
2. In your **Microsoft Edge** browser, select the **Microsoft 365 admin center** tab, and then in the left-hand navigation pane under the **Admin centers** group, select **Security**.
3. In the **Office 365 Security and Compliance** center, in the left-hand navigation pane select **Data privacy**, and then under it select **Data subject requests**.
4. In the **Data subject requests** window, select the **+New DSR case** button on the menu bar. This initiates the **New DSR case** wizard.
5. In the **Name your case** page, enter the following information and then select **Next**:
   - Name: **Holly Dickson Subject Request**
   - Description: **This is a test of the DSR resource to pull info on Holly Dickson.**
6. In the **Request details** page, select the **Data subject (the person who filed this request)** field, which displays a list of users. Select **Holly Dickson** and then select **Next**.
7. In the **Confirm your case settings** page, review your settings. If necessary, select **Edit** next to either setting to change it. If everything looks correct, select **Save**.
8. In the **Successfully created new DSR case** window, select **Show me search results**.
9. A new **Search query** window will appear and begin the query. In the detail pane on the left, scroll to the bottom, where the **Status** of the query is displayed. Wait for the status to change from **running query...** to **Completed**.

   Note: Depending on how much data is accrued, a query can take some time to complete. For Adatum's pilot project, they have not accrued much in the way of data, so Holly Dickson's query should only take a minute or so to complete.
10. While you wait for the query to complete, scroll down under **Search query** in the left-hand pane to review the default query parameters. You can modify any of the parameters and save the query for future use. If you modify any of the parameters, select **Save**.
11. Once the search query is complete, scroll through the search results and review them.

    Once you are done, select the **Home** tab at the top of the page. For Holly Dickson's case, select **Close case** to the right of the **Active** status, and then select **Yes** on the **Warning** dialog box that appears.
12. This automatically returns you to the **Searches** tab, which displays the saved search requests. Leave this window open as you resume testing in the next task from this point.

You have created a data subject request and you have searched for the personal information of Holly. At the end of your test, you have closed the DSR case again.

39.0.2 Task 2 – Export the DSR Search Query Results

When someone files a DSR, you typically must export the results for further processing, oftentimes by legal teams that must investigate a case. In this task, Holly will export the DSR report for the previous case.

1. This task will resume from where you left off previously, which was the **Searches** tab in the **Holly Dickson Data Subject Request > CoreED > Search** window. The only existing search request is the **Holly Dickson Subject Request** that you just created and ran.

   Select the check box to the left of this search; this will open the **Holly Dickson Subject Request** window.

2. In the **Holly Dickson Subject Request** window, scroll to the bottom of the window to view search statistics of the results as well as the search query syntax. After reviewing the statistics, scroll back to the top of the pane and select the **Export report** button.

   Warning: Do not select the **Export results** button. If you do not look close enough, you may accidentally select the **Export results** button rather than the **Export report** button, which will cause the export report process to fail in a later step.

3. In the **Export report** pane that appears, select the option that states: **All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons**.

   Note: Be careful - At first glance, the first two options appear to be similar; however, the first one **excludes** items while the second one **includes** those same items. Select the second option.

4. At the bottom of the **Export report** pane, select the **Generate report** button.

5. If a **Client Error** dialog box appears, select **OK**.

6. When the report finishes, scroll down through the **Holly Dickson Data Subject Request** pane to review the results, and then select the **Close** button at the bottom of the pane.

7. In the **Holly Dickson Data Subject Request > CoreED > Search** window, select the **Exports** tab from the top menu. In the list of export requests, select **Holly Dickson Subject Request_ReportsOnly** to open it.

8. In the **Holly Dickson Subject Request_ReportsOnly** pane that appears on the right, scroll down to the **Export key** section and select the **Copy to clipboard** option that appears below the export key. You will paste in this key in a few more steps.

9. At the top of the **Holly Dickson Subject Request_ReportsOnly** pane, select the **Download report** button. In the notification bar that appears at the bottom of the page, select **Open**.

10. An **Application Install – Security Warning** window will appear that wants to install the **Microsoft 365 Office 365 eDiscovery Export Tool**. Select the **Install** button.

11. When the **eDiscovery Export Tool** is installed, you need to paste in the export key that you just copied to the clipboard. In the **eDiscovery Export Tool** dialog box, select into the **Paste the export key that will be used to connect to the source** field and then press **Ctrl+V** to paste in the key.

12. Select the **Browse** button next to the **Select the location that will be used to store downloaded files** field, and in the **Browse For Folder** window, select the **Documents** folder and then select **OK**.

13. In the **eDiscovery Export Tool** window, select **Start** to begin the export process.

14. As soon as the **eDiscovery Export Tool** shows three green checkmarks with a **The export completed successfully** message below them, the export is done. Select the link that appears next to **Export Location**.

15. This opens a **File Explorer** window. Double-click the **results.csv** file to open Excel and view the report data for all DSR case items found. When you're done, close the Excel spreadsheet and then close the **File Explorer** window.

16. Close the **eDiscovery Export Tool** by selecting the **Close** button, and then close the **Holly Dickson Subject Request_ReportsOnly** window.

17. In your browser, close all tabs EXCEPT for the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab.

You have successfully exported a DSR case report to your local computer. Note: Because the report contains only a report and not the message or document content, you could not process this report to fulfill the DSR's legal requirements.

40 Proceed to Lab 8 - Exercise 2

41 Module 8 - Lab 8 - Exercise 2 - Investigate Your Microsoft 365 Data

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, you want to test how Adatum can investigate its Microsoft 365 data. You have decided to focus on performing a content search for deleted emails, which is a common request at Adatum, and then you want to analyze eDiscovery functionality by creating an eDiscovery case. You have asked Joni Sherman to conduct these tests on her client computer.

41.0.1 Task 1 – Perform a content search for deleted emails

In this exercise, you will log into Microsoft 365 on LON-CL2 as Joni Sherman, and you will perform a content search that looks for emails with the keyword **IP address**.

1. Switch to LON-CL2, where you should still be logged in as the **Admin** account, and you should be logged into **Outlook on the web** as **Joni Sherman** from a prior lab.
2. Joni needs to access the **Office 365 Security and Compliance** center. However, while she can access the Microsoft Office Home page, she does not have admin permissions; therefore, she cannot access the Microsoft 365 admin center from the Microsoft Office Home page, which means she cannot access the Security and Compliance center from the Microsoft 365 admin center. Therefore, she will have to access the **Office 365 Security and Compliance Center** directly.

   To do so, select a new tab in your Edge browser and enter the following URL in the address bar: **https://protection.office.com**.
3. In the **Office 365 Security and Compliance** center**, in the left-hand navigation pane, select **Search**, and then under it select **Content search**.

   Note: If you cannot see **Search** in the navigation pane yet, you need to reload the browser tab with the **Security and Compliance Center.**
4. On the **Content search** window, in the **Searches** tab, select **(+) Guided search** on the top menu. This will initiate the **New search** wizard.
5. On the **Name your search** page, enter **Content Search Test** in the **Name** field and then select **Next**.
6. On the **Locations** page, verify the **Specific locations** option is selected; if not, then select it now. As you scroll down through the **Locations** window, note that there are 3 groups of locations. Each group has an On/Off toggle switch, and they are all set to Off. If you select all locations or set all 3 toggle switches to On, the query will run for an hour or more.

   Since you do not have time in this lab to search all three locations, select the toggle switch for the first group of locations to turn it **On**, but leave the other two groups turned **Off**, and then select **Next**.
7. On the **Condition card** page, enter **IP address** into the **Keywords** field and then select **Finish**.
8. On the **Searches** tab, the **Search query** process will automatically start. In the **Search query** pane on the left, scroll to the bottom, where the **Status** of the query is displayed. Wait for the status to show **Completed**.

   Note: It may take a couple of minutes for the query to run and the data to be displayed in the right-hand pane. When the content search finishes, you will see all mailbox items that were created for the sensitive information test of your custom DLP policy related to IP addresses.
9. Close the **Content search** tab in your browser.
10. Leave the Security and Compliance Center tab open and continue with the next task.

You have successfully performed a content search for a specific key word across all locations of your tenant.

41.0.2 Task 2 – Create an eDiscovery case

In this task, you will create an eDiscovery case, add an In-Place Hold to the case to preserve mailbox content, and create a search to discover data from the hold. You will continue using Joni Sherman's user account. Having been assigned the eDiscovery Managers role back in Lab 1, Joni has the permissions necessary to create an eDiscovery case.

1. You should still be logged into LON-CL2 as the **Admin** account and signed into Microsoft 365 as Joni Sherman.
2. The **Office 365 Security and Compliance Center** should still be open in a tab in Microsoft Edge. If so, select that tab now. If not, then enter the following URL in the address bar: **https://protection.office.com.**
3. In the **Security and Compliance Center**, in the left-hand navigation pane, select **eDiscovery**, and then under it, select **eDiscovery**.
4. On the **eDiscovery** window, select the **(+) Create a case** button that appears above the list of cases.
5. In the **New case** window, enter **IP Address Violation** in the **Case name** field and select **Save**.
6. On the **eDiscovery** page, select the **Open** button that appears to the left of the **IP Address Violation** case.
7. On the **IP Address Violation** window, select the **Holds** tab on the menu bar.
8. Select **(+) Create** to create a new hold. This initiates the **Create a new hold** wizard.
9. On the **Name your hold** page, enter **IP Address Violation - Content** into the **Name** field and then select **Next**.
10. On the **Choose locations** page, for the **Exchange email** location, select the **Choose users, groups, or teams** link.
11. On the **Edit locations** page, select the **Choose users, groups, or teams** button.
12. On the **Exchange email** page, enter **Lynne** into the search field and then select the **Search** icon to the right of the field.
13. Scroll down on the page to see the search results. Under **Users, groups, or teams**, select the check box next to **Lynne Robbins**, and then select the **Choose** button at the bottom of the page.
14. On the **Edit locations** window, verify that one user, group, or team was added, which was Lynne Robbins. Select **Done**.
15. On the **Choose locations** page, **1 user, group, or team** is displayed to the right of **Exchange email**. Select **Next**.
16. On the **Query conditions** page, enter **IP address** into the **Keywords** box and then select **Next**.
17. On the **Review your settings** page, review the values and select **Edit** next to any that need to be modified. When you are satisfied with the settings, select the **Create this hold** button.
18. On the **IP address violation - Content** window, select **Close**.
19. This returns you to the **Holds** tab on the **IP Address violation > Core ED** page. Select the **Searches** tab from the top menu.
20. On the **Searches** tab, select the **+New search** button.
21. In the **New search** window, in the **Search query** pane on the left, enter **IP Address** in the **Keywords** field.
22. Under **Locations**, select the **Locations on hold** option.
23. Select **Save & run**.
24. In the **Save search** window, enter **IP Address Violation - Search** in the **Name** field and then select **Save**.
25. This will initiate a search query that looks for the keywords **IP Address**. In the detail pane on the left, scroll to the bottom, where the **Status** of the query is displayed. Wait for the status to show **Completed**.

Note: It may take a couple of minutes for the query to run and the data to be displayed in the right-hand pane. Once the query is finished, wait for the preview results to be displayed.

26. Close the **eDiscovery** tab in your browser.
27. Leave LON-CL2 open as well as all other browser tabs and continue with the next task.

You have now created an eDiscovery case, added an In-Place Hold to preserve mailbox content, and created a search to discover data from the hold.

42 End of Lab 8

43 Module 9 - Lab 9 - Exercise 1 - Configure the Microsoft Store for Business

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment as you deploy your pilot project. In this lab, you will work with the Microsoft Store for Business.

Important: Company employees can use the Microsoft Store app for accessing the Microsoft Store for Business. However, because it can take up to 36 hours for newly added apps to propagate to the private store and become visible in the Microsoft Store app, this lab uses a web browser to access the Microsoft Store for Business and configure Adatum's private store.

43.0.1 Task 1: Sign up for Microsoft Store for Business and perform initial configuration

In this task, you will begin by installing the Microsoft Store for Business on your LON-CL1 PC. You will then configure it so that apps from the Microsoft Store for Business will be allowed to run on devices that Windows Defender Device Guard is protecting.

1. Switch to LON-CL1, where you should still be logged in as the **Admin** and into Microsoft 365 as Holly Dickson (**holly@xxxxxZZZZZZ.onmicrosoft.com)** with a password of **Pa55w.rd**.
2. In your Edge browser, open a new tab and enter the following URL in the address bar: **https://www.microsoft.com/b store**
3. This opens the **Microsoft Store for Business**. In the top-right corner, select **Sign in**.
4. If you are automatically signed in as Holly Dickson, then proceed to the next step; otherwise, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **Sign in** window and then select **Next.**
5. On the **Microsoft Store for Business** page, in the menu bar at the top of the page, select **Shop for my group**.
6. Scroll down to the **Made by Microsoft** section and select **Show all** (which appears on the right side of the **Made by Microsoft** section).
7. In the **Made by Microsoft** page, select **Microsoft Remote Desktop.**
8. On the **Microsoft Remote Desktop** page, select **Get the app**.
9. On the **Microsoft Store for Business and Education Services Agreement** page, scroll to the bottom of the page, select the check box in which you accept the license agreement, and then select **Accept.**
10. In the **Thanks for your order** window, select **Close**.
11. On the **Microsoft Store for Business** page, on the menu bar at the top of the page, select **Manage**.
12. In the left-hand navigation pane, select **Products & services**.
13. In the **Products & Services** detail pane, scroll down and verify the following products appear: **Excel Mobile**, **Microsoft Remote Desktop**, **OneNote for Windows 10**, **PowerPoint Mobile**, **Sway**, and **Word Mobile**.

    Note: It may take a minute before all the apps appear on the page.
14. In the left-hand navigation pane, select **Settings**.

15. In the **Settings** page, on the **Shop** tab, scroll down to the **Shopping experience** section and select the **Show offline apps** toggle switch to turn it **On**.
16. On the menu bar at the top of the page, select **Adatum Corporation**. This is Adatum's private store.
17. As part of your pilot project, you want to change the name of your store to **Adatum private store**. On the **Adatum Corporation** private store page, select the **ellipsis (...)** icon that appears to the right of **Adatum Corporation** (above each of the product tiles), and in the menu that appears, select **Edit collection**.
18. On the **Edit collection** page, to the right of **Adatum Corporation**, select **Rename private store**.
19. On the **Settings** page, under the **Private store** section, to the right of **Your private store name: Adatum Corporation**, select **Change**.
20. In the **Private store** dialog box, enter **Adatum private store** and then select **Save**.

    Note the change to your private store name on the menu bar at the top of the page; instead of **Adatum Corporation**, it should now say **Adatum private store**.
21. On the menu bar, select **Adatum private store**.
22. On the **Adatum private store** page, verify that it displays the **Sway**, **OneNote for Windows 10**, **PowerPoint Mobile**, **Excel Mobile**, and **Word Mobile** apps.

    Note: Earlier when you viewed **Products and Services**, it included this list of client apps, along with Microsoft Remote Desktop app. You do not see the Microsoft Remote Desktop app in your private store because you already got the app at the start of this task.
23. Leave the **Microsoft Store for Business** tab open in your Edge browser. You will use this in the next exercise.

44 Proceed to Lab 9 - Exercise 2

45 Module 9 - Lab 9 - Exercise 2 - Manage the Microsoft Store for Business

In this exercise, you will add five apps to Adatum's company store, and you will create a collection of three apps that will also be added to the store. You will then verify how those apps appear in the company store to an Adatum employee.

45.0.1 Task 1: Add apps to your private store

1. On LON-CL1, you should still have the **Microsoft Store for Business** tab open in your Edge browser. If so, select it now; otherwise, navigate to **https://www.microsoft.com/business-store** and sign in as **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).
2. In the **Microsoft Store for Business**, you ended the previous exercise by renaming Adatum's private store and verifying the product apps that are available in it. In the menu bar at the top of the page, select **Shop for my group**.
3. In the next several steps, you are going to get five apps, all of which you will add to Adatum's company store. You will make them available in the store for other Adatum employees, but you will NOT install them yourself.

   Begin by scrolling down to the **Made by Microsoft** section and select **3D Builder.**
4. On the **3D Builder** window, select the drop-down arrow in the **License type** field and note the two options - **Online** and **Offline**. Select the **Online** option, and then select **Get the app**.
5. On the **Thanks for your order** page, select **Close**.
6. This returns you to the **3D Builder** page. Select the **ellipsis (...)** button that appears to the right of the **Install** button to view the additional actions that are available besides Install. Notice that only the **Manage** option is available.

7. Select **Shop for my group** on the menu bar, then scroll down to the **Made by Microsoft** section and select **Show all**.
8. In the **Made by Microsoft** window, select **Fresh Paint.**
9. On the **Fresh Paint** window, leave the **License type** set to **Online** and select **Get the app.**
10. On the **Thanks for your order** page, select **Close**.
11. Select **Shop for my group**, then scroll down to the **Made by Microsoft** section and select **Show all.**
12. In the **Made by Microsoft** window, select **Reader**.
13. On the **Reader** page, the **License type:** field currently displays **Online**. Select the drop-down arrow in the **License type** field and select **Offline**, and then select **Get the app.**
14. On the **Thanks for your order** page, select **Close**.
15. On the menu bar at the top of the page, select **Manage.**
16. On the **Overview** page, in the **Products and Services** tile, select **Manage apps.**
17. On the **Products and Services** page, as you scroll down through the apps, note how they all have an **Assign to People** option in their **Actions** menu - except for **Reader**, which you selected with an **Offline** license type. In the **Reader** action menu, note the **Download package for offline use** option.
18. On the menu bar at the top of the page, select **Adatum private store.**
19. Now that you have added these five individual apps to the company store, you will create a collection of apps that will be bundled together. On the **Adatum private store** page, select **+Add collection.**
20. In the **Add a collection** window, under **Give this collection a name**, enter **Collection1** in the **Enter a collection name** field.
21. Scroll down and select the **Add** button below each of the following products:
    - **Fresh Paint**
    - **Microsoft Remote Desktop**
    - **3D Builder**
22. At the bottom of the page, select **Done**.
23. By default, new apps are only visible to admins; as a result, they must be assigned visibility permissions to be seen by non-admins. So at this point in time, **Collection1** is only visible to admins.
24. In the following steps you will assign visibility permissions to other users for the **Fresh Paint**, **Microsoft Remote Desktop,** and **3D Builder** apps. On the menu bar at the top of the page, select **Manage.**
25. On the **Overview** page, in the **Products and Services** tile, select **Manage apps**.
26. On the **Products and Services** page, scroll down through the apps and select **Fresh Paint.**
27. On the **Fresh Paint** window, select **Private store availability**. Under **Choose groups of people who can see this app**, select **Everyone** (if it's not already selected).

    If you had to select **Everyone**, scroll to the top of the page where you can see a **Your changes have been saved** message at the top of the window.
28. Select the back arrow to the left of the address bar to return to the **Product and Services** page.
29. Repeat steps 26-28 for both **Microsoft Remote Desktop** and **3D Builder**.
30. Close the **Microsoft Store for Business** tab in your Edge browser. Leave the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab open for the next lab.

45.0.2 Task 2: View your private store as a company employee

In this task, you are going to sign into the Microsoft Store for Business as one of Adatum's employees, Joni Sherman. You'll then verify that when Joni navigates to Adatum's private store, she can see the 5 apps that Holly added to the private store, as well as the collection of apps that Holly created in the prior task.

1. Switch to LON-CL2 where you should be logged in as the **Admin** account, and into Microsoft 365 as **Joni Sherman**.

2. In your **Edge** browser, open a new tab and then enter the following URL in the address bar: **https://www.microsoft.com/business-store**
3. On the **Microsoft Store for Business** page, in the upper-right corner of the page, select **Sign in.**
4. If you are automatically signed in as Joni Sherman, then proceed to the next step; otherwise, enter **JoniS@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **Sign in** window and then select **Next.**
5. In the **Microsoft Store for Business**, on the menu bar at the top of the page, select **Adatum private store.**
6. In the **Adatum private store**, verify that Joni can see the following:
   - The five apps that were automatically added to the private store: **Sway, OneNote for Windows 10, PowerPoint Mobile, Excel Mobile,** and **Word Mobile**.
   - The **Collection1** app that you created in the prior task that includes: **Fresh Paint, Microsoft Remote Desktop,** and **3D Builder**.
7. In your browser, close the **Microsoft Store for Business** tab.

46 End of Lab 9

47 Module 11 - Lab 10 - Exercise 1 - Enable Device Management

In your role as Holly Dickson, Adatum's Enterprise Administrator, you have Microsoft 365 deployed in a virtualized lab environment for your pilot project. In this lab, you will manage user devices using Intune.

In this exercise you will verify that Adatum has installed the Enterprise Mobility + Security E5 product. You will then verify that it has been assigned to your test user accounts, and you will assign a license to yourself. You will then enable device management with Intune.

47.0.1 Task 1: Verify and assign Enterprise Mobility + Security licenses

In this task you will verify that Adatum has installed the Enterprise Mobility + Security E5 product and you will check how many licenses are available. You will then verify that a license has been assigned to your test user accounts, and you will assign a license to yourself.

1. Switch to LON-CL1, where you should still be logged in as the **Admin** account and into Microsoft 365 as Holly Dickson.
2. In **Microsoft Edge**, you should still have a tab open for the **Microsoft 365 admin center**; if so, select that tab now. If not, enter **https://portal.office.com**, sign in as **Holly**, and in the **Microsoft Office Home** page, select **Admin**.
3. In the **Microsoft 365 admin center**, select **Billing** in the left-hand navigation pane, and then under it, select **Licenses**.
4. On the **Licenses** page, note the number of licenses that are available with your tenant and the number that have already been assigned to user accounts for each of the available licenses. In your VM lab environment, 15 **Enterprise Mobility + Security E5** licenses were assigned to your tenant, and your lab hosting provider already assigned a license to the 10 pre-existing user accounts.

   Note how the **Office 365 E5** license also has 15 available with your tenant, but in this case, 11 of the 15 have been assigned to users. Your lab hosting provider assigned a license to each of the 10 pre-existing user accounts, and when you created Holly Dickson's user account back in lab 1, you assigned her a license as well. You did not assign Holly an **Enterprise Mobility + Security E5** license.

   In the list of licenses, select **Enterprise Mobility + Security E5**.
5. In the **Enterprise Mobility + Security E5** page, under the list of users, verify that all 10 of the pre-existing user accounts provided by your lab hosting provider have been assigned a license.

   The one user who was not assigned an **Enterprise Mobility + Security E5** license is Adatum's Enterprise Administrator, Holly Dickson. When you created Holly's user account back in Lab 1, you were instructed at that time to only assign her an Office 365 E5 license. You will now assign her an Enterprise Mobility + Security E5 license.

To assign Holly a license, select **+Assign licenses**, which appears in the menu bar above the list of users.

6. In the **Assign licenses to users** pane, select the **Enter a name or email address** field, and in the list of users that appears, select **Holly Dickson**, and then select the **Assign** button at the bottom of the pane.
7. Close the **You assigned a license to Holly Dickson** window.
8. Leave all browser tabs open for the next task.

You have now verified the available Enterprise Mobility + Security E5 licenses in your tenant and assigned an EMS E5 license to Holly.

47.0.2 Task 2: Enable device management with Intune

Devices must be managed before you can give users access to company resources or manage settings on those devices. This begins with enabling device management with Intune. With Adatum's tenant, Holly will discover that Intune has been set by default as Adatum's MDM authority.

1. You should still be logged into LON-CL1 as the **Admin** account and into Microsoft 365 as Holly Dickson.
2. In the **Microsoft 365 admin center**, in the left-hand navigation pane under the **Admin centers** group, select **Endpoint Manager**.
3. In the **Microsoft Endpoint Manager admin center**, select **Devices** in the left-hand navigation pane.
4. In the **Devices | Overview** page, the **Enrollment status** tab is displayed by default. By default, Intune has been set as Adatum's MDM authority.

   In the middle pane under the **Policy** section, select **Compliance policies**. Even though no data is currently available, review the information on the **Compliance policies | Policies** page regarding device management.
5. Select the **Back arrow** on the address bar to return to the **Devices | Overview** page. In the middle pane under the **Policy** section, select **Conditional Access**. Review the information on the **Conditional Access | Policies** page.
6. Select the **Back arrow** on the address bar to return to the **Devices | Overview** page. In the middle pane under the **Policy** section, select **Enrollment restrictions**. Review the information on the **Devices | Enrollment restrictions** page.
7. Select the **Back arrow** on the address bar to return to the **Devices | Overview** page. In the middle pane under the **Policy** section, select **Configuration profiles**. Review the information on the **Devices | Configuration profiles** page.
8. Select the **Back arrow** on the address bar to return to the **Devices | Overview** page.
9. In your Edge browser, leave all the tabs open for the next lab exercise.

You have now verified that Intune is the default MDM solution for your tenant.

48 Proceed to Lab 10 - Exercise 2

49 Module 11 - Lab 10 - Exercise 2 - Configure Azure AD for Intune

In this exercise you will activate automatic client enrollment to Intune for Mobile Device Management (MDM). This will enable you to manage mobile device access and set policies for restricting access to devices unless certain actions are adopted, such as strong passwords and screen timeouts.

49.0.1 Task 1: Integrate Azure AD with Intune

1. You should still be logged into LON-CL1 as the **Admin** and in Microsoft 365 as **Holly Dickson**.
2. In your browser, select the **Microsoft 365 admin center** tab, which should still be open; if not, navigate to **https://admin.microsoft.com.**
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane under **Admin centers**, select **Azure Active Directory**.

4. In the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory**.
5. On the **Adatum Corporation | Overview** window, in the middle pane under **Manage,** select **Mobility (MDM and MAM),** and then in the details pane on the right, select **Microsoft Intune**.

   Note: If you see a notification that automatic enrollment is available only for Azure AD Premium, press F5 to refresh the page in your web browser and then select **Microsoft Intune**.
6. On the **Configure** window, in the **MDM user scope** row, select **All**.

   Note: By setting this parameter to **All**, you are allowing all users who join their devices to Azure AD to automatically enroll them to Intune as well.
7. Below the list of MDM-related fields, select **Restore default MDM URLs** to ensure the correct URLs for client enrollment are configured.
8. In the menu bar at the top of the **Configure** window, select **Save**.
9. Leave all browser tabs open for the next task.

You have now configured your tenant so that all users can enroll their Windows 10 clients into Intune as soon they log into their devices with their Azure AD account credentials.

49.0.2 Task 2: Configure Azure AD join

In this task, you will change the default settings for users to join their devices to Adatum's Azure AD tenant.

1. In your browser, in the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory.**
2. In the **Adatum Corporation | Overview** window, in the middle section under **Manage**, select **Devices**.
3. In the **Devices | All devices** window, in the details pane on the right, verify that **LON-CL2** is displayed in the list of devices.

   Note: Back in Lab 5, you performed a task that configured Mobile Device Management (MDM) auto-enrollment; this was a prerequisite to performing a later Windows Information Protection lab. When you performed this MDM configuration lab, it automatically enrolled the devices belonging to members of the WIP Users group. At the time, Joni Sherman was logged into Microsoft 365 on LON-CL2, and since she was a member of the WIP Users group, LON-CL2 was automatically enrolled into Intune as its MDM authority.
4. In the **Devices | All devices** window, in the middle pane, select **Device settings**.
5. In the **Devices | Device settings** window, in the details pane on the right, in the **Users may join devices to Azure AD** option, verify that **All** is selected. This means that all Azure AD users can join their devices to Azure Active Directory.
6. Scroll down to the bottom of the window. Under **Additional local administrators on all Azure AD joined devices**, no local administrators are displayed. Select the **Manage Additional local administrators on all Azure AD joined devices**.

   On the **Device Administrators | Assignments** window, note that there are no additional assignments. In the next several steps, you will add a role assignment.
7. In the **Device Administrators | Assignments** window, select **+Add assignments** on the menu bar.
8. In the **Add assignments** pane on the right, select **Alex Wilber** in the list of users and then select the **Add** button at the bottom of the screen.
9. Select the **Back arrow** on the address bar to return to the **Devices | Device settings** page. Verify the **Require Multi-Factor Auth to join devices** toggle switch is set to **No**. The **Maximum number of devices per user** is currently set to **50**; select this field and in the drop-down menu that appears, select **10**.
10. On the menu bar at the top of the page, select **Save**.
11. Leave all browser tabs open for the next task.

You have changed the default settings for users to join their devices to your Azure AD tenant.

49.0.3 Task 3: Create dynamic Azure AD device group

In Azure Active Directory, you can use rules to determine group membership based on user or device properties. Dynamic membership is supported for security groups or Microsoft 365 groups. When a group membership rule is applied, user and device attributes are evaluated for matches with the membership rule. When an attribute changes for a user or device, all dynamic group rules in the organization are processed for membership changes. Users and devices are added or removed if they meet the conditions for a group. Devices can only be used in Security groups.

In this task, Holly wants to create a new Security group for enrolled devices within Adatum. This group will support dynamic membership when a device's management type is set to MDM.

1. In your browser, in the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory.**
2. In the **Adatum Corporation | Overview** window, in the middle pane under **Manage,** select **Groups**.
3. In the **Groups | All groups** window, in the details pane on the right, select **+New group** on the menu bar.
4. In the **New Group** window, enter the following information:
   - Group type: **Security**
   - Group name: **Enrolled Devices**
   - Membership type: **Dynamic Device**
   - Owner: select **no owners selected**, then in the **Add Owners** window, select **Alex Wilber** and then select the **Select** button
5. At the bottom of the **New Group** window, under **Dynamic device members**, select **Add dynamic query**.
6. In the **Dynamic membership rules** window, configure the following fields for this expression:
   - Property: select the drop-down arrow and select **managementType**
   - Operator: select the drop-down arrow and select **Equals**
   - Value: enter **MDM**
7. Select **+Add expression**. It should display the following in the **Rule syntax** field:

   (device.managementType -eq "MDM")
8. Select **Save** in the menu bar at the top of the window.
9. In the **New Group** window, select the **Create** button at the bottom of the window.
10. In the **Groups | All groups** window, the **Enrolled Devices** group should now appear in the list of groups.
11. Leave all browser tabs open for the next task.

50 Proceed to Lab 10 - Exercise 3

51 Module 11 - Lab 10 - Exercise 3 - Create Intune Policies

Many mobile device management (MDM) solutions help protect organizational data by requiring users and devices to meet certain requirements. In Intune, these requirements are referred to as compliance policies. Compliance policies define the rules and settings that users and devices must meet to be compliant. When combined with Conditional Access requirements, administrators can block users and devices that do not meet the rules.

In this exercise, you will begin by creating a noncompliance notification message template. Then when you create a compliance policy that checks the Windows 10 and later devices to ensure they are running a minimum OS version of Windows, you will assign this email notification template to the policy. If a device is running a noncompliant version of Windows, the policy will be triggered, the device will be marked as noncompliant, an email will be sent to the end user notifying them of the situation.

51.0.1 Task 1: Create a noncompliant email message template

In your role as Holly Dickson, Adatum's Enterprise Administrator, want to send an email message to any end user whose Windows 10 or later device becomes noncompliant. Before you create a compliance policy in task 2, you must first create the noncompliance email message template that you will assign to the policy.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, you should still have the **Microsoft Endpoint Manager admin center** open from the first exercise in this lab; if so, then select it now. If you closed it, then in **Microsoft 365 admin center**, under the **Admin centers** group in the left-hand navigation pane, select **Endpoint Manager**.
3. In the **Microsoft Endpoint Manager admin center**, in the left-hand navigation pane select **Endpoint security**.
4. On the **Endpoint security | Overview** page, in the middle pane under the **Manage** section, select **Device compliance**.
5. On the **Compliance policies | Policies** page, in the middle pane, select **Notifications**.
6. On the **Compliance policies | Notifications** page, in the details pane on the right select **+Create notification** on the menu bar.
7. On the **Create notification** page, note the three steps that appear at the top of the page. You are currently on the step **1 - Basics** page. In the **Name** field, enter **Noncompliant OS version**. Leave all the other options set to their default settings and select **Next**.
8. On the step **2 - Notification message templates** page, select an appropriate locale for you, enter **WARNING: Noncompliant device** in the **Subject** field. Then enter **Your Windows 10 or later device is not running a compliant version of the OS. The device has been marked as non-compliant and is now locked.**, select the checkbox for **IsDefault**. Select **Next**.
9. On the step **3 - Review + create** page, review your template settings. If any need to be corrected, select **Previous** to return to the appropriate page and make the necessary edits. If everything looks OK, select **Create**.
10. In your browser session, leave all the tabs open for the next task.

51.0.2 Task 2: Create and apply a compliance policy

In your role as Holly Dickson, Adatum's Enterprise Administrator, you will create a compliance policy that governs Windows 10 devices at Adatum Corporation. This policy will dictate what the minimum OS version that must be installed on a device in order for it to access Adatum's environment. It will also control how long a device can stay out of compliance before it's locked out from use, thereby, requiring administrator assistance to make it operational again. The policy will also control who it's assigned to, which in this case will be all devices enrolled in Microsoft Intune.

Given the problems caused at Adatum by devices that are running old versions of Windows, Holly wants to mark any device as noncompliant that is running a version of the OS that is older than version 10.0.17763.1192. Marking a device as noncompliant will lock the device. In the policy that Holly wants to create, any device running a version of Windows that is older than this version will be marked as noncompliant, and an email will be sent to the end-user notifying them of the situation.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, you should still have the **Microsoft Endpoint Manager admin center** open from the first exercise in this lab; if so, then select it now. If you closed it, then in **Microsoft 365 admin center**, under the **Admin centers** group in the left-hand navigation pane, select **Endpoint Manager**.
3. In the **Microsoft Endpoint Manager admin center**, in the left-hand navigation pane select **Devices**.
4. In the **Devices | Overview** window, in the middle pane under the **Policy** section, select **Compliance policies**.
5. On the **Compliance policies | Policies** window, in the details pane on the right, select **+Create Policy** on the menu bar.
6. On the **Create a policy** pane that appears, select the **Platform** field, and in the drop-down menu that appears, select **Windows 10 and later**. Select **Create**.

7. On the **Windows 10 compliance policy** window, note the five steps that appear at the top of the page. You are currently on the step **1 - Basics** page. Enter **Compliance1** in the **Name** field and then select **Next**.

8. On the step **2 - Compliance settings** page, select **Device Health** to expand it. Review the available settings and then select **Device Health** again to collapse it.

9. On the step **2 - Compliance settings** page, select **Device Properties** to expand it. In the **Minimum OS version** field, enter **10.0.17763.1192** and then note the check mark that appears on the right side of the field. Select **Device Properties** again to collapse the section.

10. On the step **2 - Compliance settings** page, expand the remaining sections and review them, and then when you are done, select **Next**.

11. On the step **3 - Actions for noncompliance** page, you can create a list of actions that you want taken when a device becomes noncompliant. One default action is already defined (**Mark device noncompliant**); this action cannot be changed or deleted. This action is scheduled to be performed **Immediately** (which means, on the day the device becomes noncompliant, which is 0 days after noncompliance).

    In addition to marking the device as noncompliant, Holly also wants to notify the end user with an email. In the **Action** column, under the **Mark device compliant** action, selecty the action field. In the drop-down arrow that appears, select **Send email to end user**.

    Leave the **Schedule (days after noncompliance)** field set to 0.

    Under the **Message template** column, select **None selected**. In the **Notification message templates** pane that appears, select **Noncompliant OS version** and then select the **Select** button.

    Note: You will not send the email to any additional recipients. If you select **None selected** under the **Additional recipients** column, you will have to select an Azure AD group to send the email to (you cannot select an individual user). Other than the end user who owns the device, Holly does not want to notify any other group, so you will not define any additional recipients.

    Note: To the far right of the **Send email to end user** row is an ellipsis icon. If you select this icon, you can select the option to Delete this action if you decide you no longer want to include it in this policy. You want to send the email notification, so do not select this Delete option.

12. Select **Next**.

13. On the step **4 - Assignments** page, you want to assign this policy to all the devices in the **Enrolled devices** group, which you created in the prior exercise.

    In the **Assignments** tab under the **Included groups** section, select **Add groups**. In the **Select groups to include** pane that appears, select **Enrolled devices** and then select the **Select** button at the bottom of the pane. Select **Next**.

14. On the step **5 - Review + create** page, review the policy settings. If anything needs to be fixed, select **Previous** and make the necessary corrections. However, if everything looks correct, select **Create**.

15. In your **Edge** browser, select the **Azure Active Directory admin center** tab. If you closed this tab at the end of the prior exercise, then in the **Microsoft 365 admin center**, in the left-hand pane under **Admin centers**, select **Azure Active Directory**.

16. In the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory**.

17. In the **Adatum Corporation | Overview** window, in the middle pane under **Manage**, scroll down and select **Mobility (MDM and MAM).**

18. In the **Adatum Corporation | Mobility (MDM and MAM)** window, in the pane on the right, select **Microsoft Intune.**

19. In the **Configure** window, in the **MAM User scope** setting, select **All**.

20. Select **Save** in the menu bar at the top of the window, and then select the **X** in the upper right corner to close the **Configure** window.

21. Leave all browser tabs open for the next task.

51.0.3 Task 3: Manually create an EFS DRA Certificate

EFS, which is the Encrypted File System that is built into Windows, allows anyone to encrypt a file. The encryption is done using digital certificates, and as part of that process, Windows assigns a Data Recovery Agent (DRA). A data recovery agent is a Microsoft Windows user who has been granted the right to decrypt data that was encrypted by other users. The assignment of DRA rights to an approved individual provides an IT department with a way to unlock encrypted data in case of an emergency. Data Recovery Agents can be defined at the domain, site, organizational unit, or local machine level. In a small to mid-sized business, the network administrator is often the designated DRA.

In very simple terms, the network administrator uses Microsoft Windows Group Policy in Active Directory to assign everyone a public key for encryption and their own personal private key for decryption. This ensures that users can only decrypt the content they have created. The data recovery agent, however, is assigned a private key capable of unlocking all content encrypted with the public key.

The administrator must generate a Data Recovery Agent certificate which grants the user permission to access the encrypted resources. However, if the DRA certificate is created after the encryption of the resource, the resource cannot be decrypted by the DRA certificate. If you don't already have an EFS DRA certificate, you'll need to create and extract one from your system before you can use Windows Information Protection (WIP).

In this task, you're going to run a command prompt in which you enter the cipher command with a /R parameter. By default, /R creates a 2048 bit RSA recovery key and a DRA certificate; the recovery key is then written to a .PFX file, and the DRA certificate is written to a .CER file. An administrator can then add the contents of the .CER file to the EFS recovery policy to create the recovery key for users and import the .PFX file to recover individual files. The files will be stored in the C:\Users\Admin folder.

The purpose of this task is to create this RSA recovery key so that if the device on which they reside becomes compromised, you can recover the files with this DRA certificate from Intune.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In the Search field on the taskbar at the bottom of the screen, enter **cmd,** and in the menu that appears, select **Command Prompt**.
3. In the **Command Prompt** window, you are going to enter a **cipher** command, which displays or alters the encryption of file directories on NTFS partitions. The **/R** parameter generate an EFS recovery key and a DRA certificate and then stores them in two respective files (for the purpose of this lab, you're going to name each file **DRAcert**; in the real-world, you can name them whatever you wish). The EFS recovery key will be written to a **DRAcert.PFX** file, and the certificate to a **DRAcert.CER** file.

   At the command prompt, enter the following command and press Enter:

   cipher /R:DRAcert
4. You will be prompted to type in a password to protect your .PFX file. Enter **Pa55w.rd** and press Enter.

   Note: The cursor will NOT move when you type in the password, so you will not see what you're typing. You should also write down the password for future use; you will need this in a later task when you try to recover an encrypted file.
5. You will be prompted to type in the password again to confirm it. Press Enter when done.

   Note: If the password and confirmation password did not match, you must repeat the prior two steps.
6. If the password and confirmation password match, you will receive messages indicating that your .CER and .PFX files were created successfully.
7. Close the Command Prompt window.
8. Leave all browser tabs open for the next task.

51.0.4 Task 4: Create an App Protection Policy

In your role as Holly Dickson, Adatum's Enterprise Administrator, you are now going to create an app protection policy that will protect selected applications from intrusion. In other words, the apps will be protected so that they can only be accessed by individuals who are authorized to do so, such as Adatum employees and other users from your Microsoft 365 tenant. This enables you to use Windows Information Protection (WIP) policies with Windows 10 apps to protect apps without device enrollment.

In this task, you will create a WIP policy that protects an entire collection of recommended apps, as well as an app from the Microsoft Store, which in this case is **Microsoft Power BI**. Since this app produces reports and queries of company trends that may be confidential, Adatum wants to restrict access to it to selected individuals.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, you should have a tab open in the **Microsoft Endpoint Manager admin center** that is displaying the **Compliance1** data compliance policy that you created in the earlier task.

   In the left-hand navigation pane, select **Apps**.
3. In the **Apps | Overview** window, in the left-hand pane under the **Policy** group, select **App Protection policies**.
4. In the **Apps | App protection policies** window, in the menu bar that appears above the list of policies, select **+Create policy.** In the drop-down menu that appears, select **Windows 10**.
5. On the **Create policy** window, note the six steps that appear at the top of the page. You are currently in the step **1 - Basics** page. Enter the following information:

   - Name: **Win10Policy**
   - Description: **Windows Information Protection policy for Windows 10 computers**
   - Enrollment state. **With Enrollment**
6. Select **Next**.
7. On the step **2 - Targeted apps** page, under the **Protected apps** group, select **+Add**.
8. In the **Add apps** pane that appears on the right, select the drop-down arrow in the field that currently displays **Recommended apps**. The drop-down menu that appears displays the available app options that you can add to this policy - **Recommended apps, Store apps**, and **Desktop apps**. Since you're first going to add all the recommended apps, select **Recommended apps**.

   The quickest way to add all the recommended apps is to select the check box to the left of the **Name** column heading; this will select the check boxes for all the apps in the list. Select the **OK** button at the bottom of the window.
9. This returns you to the step **2 - Targeted apps** page. Scroll down past all the recommended apps that you just added and then select **+Add** again.
10. In the **Add apps** pane, you're going to add **Microsoft Power BI**, which is an app from the Microsoft Store. Select the drop-down arrow in the field that currently displays **Recommended apps**, and in the menu that appears, select **Store apps**.
11. In the **Add apps** window, enter the following information and then select **OK**:

    - Name: **Microsoft Power BI**
    - Publisher: **CN=Microsoft Corporation, o=Microsoft Corporation, L=Redmond, S=Washington, C=US**
    - Product Name: **Microsoft.microsoftpowerBIforWindows**
12. Select **OK** to close the **Add apps** pane, and then select **Next**.
13. On the step **3 - Required settings** page, in the **Windows Information Protection mode** setting, select **Block**, and then select **Next**.

    Note: By choosing the **Block** setting, WIP will look for inappropriate data sharing practices and stop the user from completing the action. Blocked actions can include sharing information across non-corporate-protected apps and sharing corporate data between other people and devices outside the organization. Holly has decided to select this option given her concern over the Microsoft Power BI app, which can produce reports and queries of company trends that may be confidential.
14. On the step **4 - Advanced settings** page, scroll down to the **Data protection** section. You will upload the DRA certificate that you created in the prior task, which will allow recovery of encrypted data.

    To the right of the **Select a file** field, select the **file** icon. In the **File Explorer** window that appears, expand **Local Disk (C:)**, expand **Users**, and then select the **Admin** folder. Scroll down through the files in the **Admin** folder, select **DRAcert.CER**, and then select **Open**.

Note: DRAcert.CER should now appear in the certificate field in the **Data protection** section. The DRAcert certificate has now been uploaded to the App Protection policy titled **Win10Policy**. This certificate is now available for use in unencrypting protected files.

Important: At this point in a real-world scenario, to maintain device integrity, you should copy your data recovery certificate to an offline location on a thumb drive or stored in a program for keys and passwords. You should also create a backup of this file and store it at another location. The certification is how you recover files using Intune. If the certificate is not saved, then you cannot recover the file using Windows Information Protection if the device ever becomes compromised. For this lab, you will not store the certificate to an offline device.

15. Select **Next**.
16. On the step **5 - Assignments** page, under **Included groups**, select **Add groups**. Holly wants to limit this policy to the members of the **WIP Users** group, which is the group of users selected to participate in compliance testing for Adatum's pilot project.

    In the **Select groups to include** pane, select **WIP users**, and then select the **Select** button at the bottom of the pane.
17. Select **Next**.
18. On the step **6 - Review + create** page, review the policy settings. If anything needs to be fixed, select **Previous** and make the necessary corrections. However, if everything looks correct, select **Create**.
19. On the **Apps | App protection policies** window, **Win10Policy** should appear in the list of policies. However, note that its **Deployed** status is **No**. It only takes a few seconds for the policy to be deployed, so select **Refresh** on the menu bar and the **Deployed** status should change to **Yes**.
20. Leave all browser tabs open for the next task.

You have just created a new App Protection Policy (APP), which is also referred to as a Windows Information Protection (WIP) policy.

51.0.5 Task 5: Create a packaged App rule for the store apps

Packaged apps, also known as Universal Windows apps, are based on an app model that ensures that all the files within an app package share the same identity. Therefore, it is possible to control the entire app using a single AppLocker rule as opposed to the non-packaged apps where each file within the app could have a unique identity. An AppLocker rule for a packaged app controls both the installation as well as the running of the app.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In the Search field on the taskbar at the bottom of the screen, enter **SecPol** and in the menu that appears, select **Local Security Policy**.
3. In the **Local Security Policy** window, in the left-hand pane, expand **Application Control Policies**, expand **Applocker**, and then select **Packaged app Rules**. In the menu bar at the top of the window, select **Action** and then in the drop-down menu that appears, select **Create New Rule.**
4. This starts the **Create Packaged app Rules** wizard. On the **Before You Begin** page, select **Next.**
5. On the **Permissions** page, make sure the **Action** option is set to **Allow** and the **User or group** is set to **Everyone**, and then select **Next**.
6. On the **Publisher** page, under the **Use an installed packaged app as a reference** option, select the **Select...** button.

   Note: It may take around 30 seconds for the **Select applications** window to appear.
7. In the **Select applications** window, pick the app that you want to use as the reference for your rule. For this lab, enter **one** in the **Search** field, and then in the list of results, select the check box to the left of **OneNote**. Select **OK**.
8. On the **Publisher** page, select the **Create** button at the bottom of the page.
9. If a dialog box appears asking whether you want to create default rules, select **No**. You must not create default rules for your WIP policy.
10. In the **Local Security Policy** window, in the left-hand pane, right-click on **AppLocker** and select **Export policy.**

11. In the **Export policy** File Explorer window, you will export and save your new policy as an XML file. Select the **Documents** folder, enter **apprule1** in the **File name** field, verify the **Save as type** field displays **XML (*.xml)**, and then select **Save**.
12. An **AppLocker** dialog box appears displaying a message that **1 rules were exported from the policy**. Select **OK.**
13. In the **Local Security Policy** window, under **AppLocker**, select **Executable Rules**, and then right-click on **Executable Rules**. In the menu that appears, select **Create New Rule.**
14. On the **Before You Begin** page, select **Next.**
15. On the **Permissions** page, make sure the **Action** option is set to **Allow** and the **User or group** is set to **Everyone**, and then select **Next.**
16. On the **Conditions** page, select the **Path** option and then select **Next**.
17. On the **Path** page, select the **Browse Folders....** button (do not confuse this with the **Browse Files** button).
18. In the **Browse For Folder** window, select **Local Disk (C:)**, select **Program Files**, and then select **OK**. Select **Next**.
19. On the **Exceptions** page, you are not adding any exceptions, so select **Next**.
20. On the **Name and Description** page, select the **Name** field, replace the existing content by entering **exerule1**, and then select **Create**.
21. If an **AppLocker** dialog box appears asking if you want to create the default rules, select **No**.
22. In the **Local Security Policy** window, in the left-hand pane, right-click on **AppLocker** and select **Export policy.**
23. In the **Export policy** File Explorer window, you will export and save your new policy as an XML file. Select the **Documents** folder, enter **exerule1** in the **File name** field, verify the **Save as type** field displays **XML (*.xml)**, and then select **Save**.
24. An **AppLocker** dialog box appears displaying a message that **2 rules were exported from the policy**. Select **OK.**
25. Close the Local Security Policy window.
26. After you've created your XML files, you will import one of them by using **Microsoft Intune**, which you will do in the next task.

51.0.6 Task 6: Import a list of protected apps using Endpoint Manager

The purpose of this task is to show you how to use Intune to push an app to a device just like a Group Policy Object (GPO). In this task, you will use Notepad. In a previous task, Notepad was included as one of the recommended apps in the App protection policy that you created. In this task you will import into Intune the App protection policy (**apprule1.xml**) that you exported in the prior task.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, you should have the **Microsoft Endpoint Manager admin center** portal open in a tab titled **Apps - Microsoft Endpoint Manager admin center**. Select this tab.
3. In the **Apps – App protection policies** window, it displays the list of app protection policies. In this list, select **Win10Policy**.
4. In the **Intune App Protection** window, in the middle pane under **Manage**, select **Properties**.
5. In the **Intune App Protection | Properties** window, the detail pane displays the Intune App Protection properties by group (for example, Basics, Targeted apps, Required settings, and so on). Select **Edit** that appears next to the **Targeted apps** group.
6. In the **Edit policy** window, scroll down past the list of Protected apps and then select **+Import**.
7. In the **Import apps** pane that appears, select the folder icon that appears to the right of the **Select a file** field.

8. In the **File Explorer** window that appears, select the **Documents** folder, select the **apprule1.xml** file, select **Open**, and then at the bottom of the **Import apps** pane, select **OK**.

   Note: This imports the file, and the apps are added to your **Protected apps** list.

9. On the **Edit policy** window, select the **Review + save** button that appears at the bottom of the window, and then select **Save**.
10. You now want to create a file that you're going to encrypt using Windows Information Protection. In the search field on your taskbar, enter **Notepad**, and then in the menu, select **Notepad**.
11. In the **Notepad** window, enter **This is a WIP encryption test** and then select **File**, select **Save as,** select the **Documents** folder, enter **apptest1** as the **File name**, and then select **Save.**
12. Close Notepad.
13. In the search field on your taskbar, enter **cmd**, and then in the menu, right-click on **Command Prompt** and select **Run as administrator**.
14. In the **Command Prompt** window, at the prompt, enter the following command to encrypt the apptest1.txt file (the /e parameter directs the cipher command to encrypt the file):

    cipher /e C:\Users\Admin\Documents\apptest1.txt

15. Leave the Command Prompt window open for the next task, but minimize it for now.

51.0.7 Task 7: Recover data using the EFS DRA certificate

The purpose of this task is to show you how to recover a file that has been encrypted using WIP if the Windows 10 device on which it resides has been recovered after having been misplaced or stolen. In this case, you will decrypt the apptest1.txt file that you earlier encrypted. In a real-world scenario, you would start out by copying your WIP-encrypted file to a location where you have admin access; however, in this lab, we're simply going to point to the apptest1.txt file to keep things simple.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. You must now install the **DRAcert.PFX** file. To do so, select the **File Explorer** icon on the taskbar at the bottom of the screen. Maximize the **File Explorer** window.
3. In **File Explorer**, expand **Local Disk (C:)**, expand **Users**, and select **Admin**.
4. In the list of files in the **Admin** folder, double-click on the **DRAcert.PFX** file. This initiates the **Certificate Import Wizard**.
5. On the **Welcome to the Certificate Import Wizard** page, select the **Current User** option and then select **Next**.
6. On the **File to import** page, select **Next.**
7. On the **Private key protection** page, in the **Password** field, enter the password that you assigned to the DRAcert file that you created in Task 2 (in a real-world scenario, you were instructed to write this down for future use). For this lab, enter **Pa55w.rd**, which was the password that you assigned to the DRAcert file. To verify what you typed, select the **Display Password** check box. Select **Next**.
8. On the **Certificate store** page, select **Next.**
9. On the **Completing the Certificate Import Wizard** page, select **Finish.**
10. On the **Import was successful** dialog box, select **OK**.
11. You should still have a **Command Prompt** window open from the previous task. Select the **Command Prompt** icon on the taskbar to display the window. If you closed the Command Prompt window at the end of the prior task, then open a command prompt with elevated rights.
12. In the Command Prompt window, run the following command to decrypt the apptest1.txt file (the /d parameter directs the cipher command to decrypt the file):

    cipher /d C:\Users\Admin\Documents\apptest1.txt

    A message should be displayed in the Command Prompt window indicating one file was decrypted.

13. Close the Command Prompt and File Explorer windows.

14. Leave all browser tabs open for the next task.

51.0.8 Task 8: Configure enrollment restrictions

When enrolling devices to Microsoft Intune, you have the option to Allow or Block personally owned devices from being enrolled. This is done by restricting what device type platforms you want to allow when devices are enrolled. For example, if you configured Intune to only allow iOS devices to be enrolled and a user attempts to enroll an Android device, the operation would be blocked from enrolling.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, you should have a tab open for the **Microsoft Endpoint Manager admin center** that's displaying the **Intune App Protection | Properties** window. In the left-hand navigation pane, select **Devices**.
3. In the **Devices| Overview** window, in the middle pane under the **Device enrollment** section, select **Enroll devices.**
4. In the **Enroll devices | Windows enrollment** window, in the middle pane, select **Enrollment restrictions**.
5. In the **Enroll devices | Enrollment restrictions** window, in the details pane on the right, in the **Device type restrictions** section, on the **Default** restriction type, select **All users**.
6. In the **All Users** window, in the middle pane under the **Manage** section, select **Properties.**
7. In the **All Users | Properties** window, select **Edit** that appears next to **Platform settings**.
8. In the **Edit restriction** window, under the **Platform** column, select **Block** for the **iOS/iPadOS** and **macOS** types, select the **Review + save** button at the bottom of the screen, and then review your changes. Both platform settings should display **Block (edited)** under the **Platform** column. All other device types should be allowed. Select **Save.**
9. In the navigation thread at the top of the page (**Home > Devices > Enroll devices > All users**), select **Enroll devices**.
10. In the **Enroll devices | Enrollment restrictions** window, in the **Device limit restrictions** section, on the **Default** row, select **All users**.
11. In the **All Users** window, in the middle pane under the **Manage** section, select **Properties.**
12. In the **All Users | Properties** window, select **Edit** that appears next to **Device limit**.
13. In the **Edit restriction** window, select the **Device limit** field, in the drop-down menu select **3**, and then select **Review + save.** Review your change and then select **Save.**
14. Leave all browser tabs open for the next task.

51.0.9 Task 9: Review device configuration profiles

The purpose of this task is to simply review the different platforms that are available to be assigned to a device configuration profile. You will not create a profile; you will simply review the platforms that are available to assign to a profile.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, you should have a tab open for the **Microsoft Endpoint Manager admin center** that's displaying the **All Users | Properties** window. In the left-hand navigation pane, select **Devices**.
3. On the **Devices | Overview** window, in the middle pane under **Policy,** select **Configuration profiles**.
4. On the **Devices |Configuration profiles** page, select **+Create profile** that appears on the menu bar above the list of profiles.
5. On the **Create a profile** pane, select the **Platform** field to see the different platforms that are available. **Do not select any option.** The purpose of this task is to simply see what platforms are available that can be assigned to a new device profile, should you want to ever create one.
6. Close the **Create a profile** pane.
7. Leave all browser tabs open for the next lab exercise.

52 Proceed to Lab 10 - Exercise 4

53 Module 11 - Lab 10 - Exercise 4 - Enroll a Windows 10 Device

One of Adatum's goals for their Microsoft 365 deployment is to enroll their Windows 10 devices to Microsoft Intune so that the devices can be managed by MDM. As part of her pilot project, Holly Dickson wants to enroll the LON-CL1 PC to Intune. In this exercise, you will first verify that the device is not currently enrolled, and having done that, you will enroll the device to Azure AD and Intune and then verify the enrollment.

During her pilot project, Holly plans to use certificates with Intune to authenticate Adatum's users to applications and corporate resources through VPN, Wi-Fi, and email profiles. By using certificates to authenticate these connections, Adatum's end-users won't need to enter usernames and passwords, which helps to make their access seamless.

53.0.1 Task 1: Verify the device is not enrolled

Holly must begin by verifying that the device she wants to enroll into Intune (LON-CL1) is not already enrolled.

1. You should still be logged into LON-CL1 as the **Admin** and into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, the **Microsoft Endpoint Manger admin center** should still be open in the **Devices - Microsoft Endpoint Manager admin center** tab. Select this tab.
3. In the **Microsoft Endpoint Manger admin center**, in the left-hand navigation pane, select **Devices**.
4. In the **Devices | Overview** window, in the middle pane, select **All devices**.
5. In the **Devices | All devices** window, verify that LON-CL2 is the only device listed in the details pane. You have just verified that LON-CL1 is not enrolled into Intune.

   Note: LON-CL2 was enrolled into Intune in an earlier lab when you configured integration between Azure AD and Intune. When you joined LON-CL2 to Azure AD, it was automatically enrolled to Intune.
6. You now want to start the **Certificates** MMC for LON-CL1. In the Search field on the taskbar, enter **run**, and then in the list of search results, select **Run**.
7. In the **Run** window, enter **certlm.msc** in the **Open** field and then select **OK**. If a **Do you want to allow this app to make changes to your device?** dialog box appears, select **Yes**.
8. Maximize the **certlm – [Certificates – Local Computer]** window that appears and then drag the pane divider to the right so that you can see the entirety of the left-hand pane.
9. In the left-hand pane, select **Personal** and then select the **Certificates** child folder under the **Personal** folder. Verify that only the localhost certificate appears.
10. Minimize the **certlm – [Certificates – Local Computer]** window as you will use it in a later task.

53.0.2 Task 2: Enroll the device to Azure AD and Intune

In this task, you want to enroll LON-CL1 to Azure AD and Intune.

1. In **LON-CL1**, enter **access work** in the Search field on the taskbar, and then in the list of search results, select **Access work or school**.
2. In the **Settings** app, in the **Access work or school** section, select **+Connect**.
3. In the **Microsoft account** window, on the **Set up a work or school account** page, select **Join this device to Azure Active Directory**.
4. On the **Let's get you signed in** page, in the **Work or school account** text box, enter **Holly@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next**.
5. On the **Enter password** page, enter **Pa55w.rd** in the **Password** field and then select **Sign in**.
6. On the **Make sure this is your organization** dialog box, review the information and if everything looks correct, select **Join**.
7. On the **You're all set!** page, select **Done**.

8. In the **Settings** app, close the **Access work or school** page by selecting the **X** in the upper right-hand corner.
9. In your Edge browser, in your **Microsoft Endpoint Manager admin center**, the **Devices | All devices** page should still be displayed. Currently it displays only LON-CL2. Select **Refresh** on the menu bar at the top of the detail pane. Verify that **LON-CL1** appears in the list of devices along with **LON-CL2**.

   You should also note that in the list of devices, LON-CL1 was identified as Corporate-owned device, whereas LON-CL2 was identified as a Personal device. Since LON-CL1 was enrolled by Holly, an administrator, LON-CL1 is classified as a Corporate device. Conversely, since Joni Sherman, a non-administrator, enrolled LON-CL2, device ownership is classified as a Personal device. D
10. Leave all browser tabs open for the next task.

53.0.3 Task 3: Verify the device is enrolled to Azure AD and Intune

In an earlier lab you configured integration between Azure AD and Intune. Because of that, any device that is joined to Azure AD is automatically enrolled to Intune. In this task you will join LON-CL2 to Azure AD, which will automatically enroll it into Intune.

1. You should still be logged into **LON-CL1** as the **Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In **LON-CL1**, select the **certlm – [Certificates – Local Computer]** icon on the taskbar.
3. In the **certlm – [Certificates – Local Computer]** console, in the left-hand navigation pane, the **Personal > Certificates** folder should already be selected from the earlier task. In the menu bar, select **Action** and then select **Refresh**. In the details pane, verify that several certificates appear along with the **localhost** certificate, which was the only certificate originally in this folder.

   Note: These certificates were added when you joined the LON-CL1 device to Azure AD, which in turn enrolled it to Intune.
4. Close the **certlm – [Certificates – Local Computer]** window.
5. In your **Edge** browser, select the **Azure Active Directory** tab.
6. In the **Azure Active Directory admin center**, in the left-hand navigation pane, select **Azure Active Directory**.
7. In the **Adatum Corporation | Overview** page, in the middle pane under the **Manage** section, select **Devices**.
8. In the **Devices | All devices** page, both **LON-CL1** and **LON-CL2** should be displayed. Drag the horizontal scroll bar to the right until the **MDM** column is visible. Note that both devices are enrolled to **Microsoft Intune**.

   Note: This view lists devices that are joined to Azure AD. Remember that you configured integration between Azure AD and Intune, and because of that, any device that is joined to Azure AD is automatically enrolled to Intune.
9. Leave all browser tabs open for the next task.

54 Proceed to Lab 4 - Exercise 5

55 Module 11 - Lab 10 - Exercise 5 - Manage and Monitor a Device in Intune

Holly Dickson wants to make managing devices easier, so she has decided to implement Microsoft Intune device categories in her pilot project. Implementing device categories will enable her to automatically add devices to groups based on categories that she defines.

As part of managing devices in Intune, Holly will create dynamic groups in the Microsoft Endpoint Manager admin center, based on the device category and device category name. After you configure device groups, users who enroll their device will be presented with a list of the categories you configured. After they choose a

category and finish enrollment, their device is added to the Active Directory security group that corresponds with the category they chose.

55.0.1 Task 1: Create device categories

In this task, you're going to create two device categories, one for mobile devices and the other for desktop systems. These categories will then be assigned to devices in the next task.

1. In the LON-CL1 VM, you should still be logged in as the **Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, the **Microsoft Endpoint Manager admin center** should still be open. In the left-hand navigation pane, select **Devices**.
3. In the **Devices | Overview** window, in the middle pane under the **Other** section, select **Device categories.**
4. In the **Devices | Device categories** window, select **+Create device category**.
5. On the **Create device category** window, the top of the page shows the 3 steps involved in creating a device category. In step **1 - Basics**, enter **Mobile Device** in the **Name** field and then select **Next**.
6. On the step **2 - Scope tags** window, you will not define any scope tags, so select **Next**.
7. On the step **3 - Review + create** window, select **Create**.
8. Repeat steps 4-7 to create a second device category, this one titled **Desktop**.
9. Leave all browser tabs open for the next task.

55.0.2 Task 2: Manage the enrolled devices

In this task, you're going to manage the Category property of the two devices that are joined to Azure AD and enrolled in Microsoft Intune. You will also review the properties and discovered apps on each device.

1. In the LON-CL1 VM, you should still be logged in as the **Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. In your Edge browser, the **Microsoft Endpoint Manager admin center** should still be open and it should be displaying the **Devices | Device categories** window after having completed the prior task.
3. In the **Devices | Device categories** window, scroll to the top of the middle pane and select **All devices**.
4. On the **Devices | All devices** window, select **LON-CL1**, which is the device that Holly joined to Azure AD, and which was automatically enrolled to Intune.
5. On the **LON-CL1** window, review the device details. Also review the actions available on the menu bar at the top of the page; these are the actions that you can perform against the device.
6. On the **LON-CL1** window, in the left-hand pane under the **Manage** section, select **Properties**.
7. In the **LON-CL1 | Properties** window, note the current value of the **Device category** field is **Unassigned**. Select the drop-down arrow for this field and in the menu, note the appearance of the two device categories (Mobile Device and Desktop) that you created in the prior task. Select **Desktop**, and then on the menu bar at the top of the page, select **Save**.

   Note: For Android or iOS devices, you must select the **Device category** during enrollment.
8. In the **LON-CL1 | Properties** window, in the left-hand pane under the **Monitor** section, select **Hardware.**
9. In the **LON-CL1 | Hardware** window, review the hardware information that synced from the device. Then scroll down and review the **Conditional access** section at the bottom of the page.
10. In the left-hand pane under the **Monitor** section, select **Discovered apps** and review the list of apps that were discovered on the device.
11. In the **LON-CL1 | Discovered apps** window, note the navigation thread at the top of the windows (**Dashboard > Devices > LON-CL1**). Select **Devices** in this thread. This returns you to the **Devices | All devices** window.

12. Repeat steps 4-10, but this time select **LON-CL2**, which is the device that Joni Sherman joined to Azure AD in an earlier lab. Change the **Device category** value to **Mobile Device**.
13. Leave all browser tabs open for the next task.

55.0.3 Task 3: Create dynamic groups for the device categories

1. In your Edge browser, the **Microsoft Endpoint Manager admin center** should still be open. In the left-hand navigation pane, select **Groups**.
2. In the **Groups** window, select **+New group** on the menu bar.
3. In the **New Group** window, enter the following information:
   - Group type: **Security**
   - Group name: **Mobile Devices**
   - Membership type: **Dynamic Device**
4. Under the **Dynamic device members** section, select **Add dynamic query**.
5. On the **Dynamic membership rules** window, hover your mouse over the row to display the rule fields, and then enter the following values:
   - Property: **deviceCategory**
   - Operator: **Equals**
   - Value: enter **Mobile Device** (Note: This must match the spelling of the corresponding category that you created, which in this case is Mobile Device)
6. Select in the **Rule syntax** field and the query syntax will appear.
7. Select **Save** on the menu bar at the top of the page.
8. On the **New Group** window, select the **Create** button at the bottom of the page. The **Mobile Devices** group should now appear in the list of groups.
9. Repeat steps 2-8 to create a group for desktop devices. The **Group Name** should be set to **Desktop Devices**, and in the **Dynamic membership rules** window, enter **Desktop** in the **Value** field.
10. In the **Groups | All groups** window, both new groups should appear at the top of the group list.
11. Leave all browser tabs open for the next task.

55.0.4 Task 4: Create a conditional access policy

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions.

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity-driven control plane.

In this task, you will create a conditional access policy that Holly plans to implement in her pilot project.

1. In your Edge browser, the **Microsoft Endpoint Manager admin center** should still be open. In the left-hand navigation pane, select **Endpoint Security**.
2. In the **Endpoint security | Overview** window, in the middle pane under the **Manage** section, select **Conditional access**.
3. In the **Conditional Access | Policies** window, select **+New policy** on the menu bar.
4. On the **New** pane, in the **Name** field, enter **Conditional1** and then select the **Users and groups** section.
5. On the **Users and groups** pane, select the **All users** option.
6. On the **New** pane, select the **Cloud apps or actions** section.
7. On the **Cloud apps or actions** pane, select the **Select apps** option.
8. In the **Select** pane that appears, enter **Exchange** in the Search field. In the list of search results, select the check box for **Office 365 Exchange Online**, and then select the **Select** button at the bottom of the pane.

9. On the **New** pane, select the **Conditions** section.
10. On the **Conditions** pane, select the **Device platforms** section.
11. On the **Device platforms** pane that appears, in the **Configure** field, select **Yes**. In the **Include** tab, select the **Select device platforms** option and then select the **Windows** check box. Select **Done**.
12. On the **New** pane, under **Access Controls**, select the **Grant** section.
13. On the **Grant** pane that appears, select the **Require device to be marked as compliant** check box, and then select the **Select** button.
14. On the **New** pane, under **Access Controls**, select the **Session** section.
15. In the **Session** pane that appears, review the explanation but do not select any option. Select the **X** in upper right corner to close the pane.
16. On the **New** pane, select the **Create** button at the bottom of the pane. The **Conditional1** policy now appears in the policy list.
17. You created a conditional access policy to become familiar with the available options; however, the policy is not effective because you didn't enable it. To enable the policy, select the **Conditional1** policy in the policy list.
18. In the **Conditional1** pane, the **Enable policy** setting appears at the bottom of the pane. By default, it's set to **Report-only**. Select **On** and then select **Save**.

You have now created a conditional access policy and enabled it for Adatum's pilot project.

56 End of Lab 10