Contents

1 INF99X: Sample Course **3**
- 1.1 What are we doing? . . . 3
- 1.2 How should I use these files relative to the released MOC files? . . . 3
- 1.3 What about changes to the student handbook? . . . 3
- 1.4 How do I contribute? . . . 3
- 1.5 Notes . . . 4
  - 1.5.1 Classroom Materials . . . 4
- 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. . . . 4
- 1.7 title: Online Hosted Instructions permalink: index.html layout: home . . . 4

2 Content Directory **4**
- 2.1 Labs . . . 4
- 2.2 Demos . . . 4

3 Module 10 - Lab 9 - Exercise 1 - Prepare Azure AD for Hybrid Synchronization **4**
- 3.1 Task 1: Configure your tenant to support local mail transport . . . 5
- 3.2 Task 2: Create a Custom Domain in Microsoft 365 . . . 5
- 3.3 Task 3: Configure the UPN name for custom domain . . . 11
- 3.4 Task 4: Enable Exchange for the Custom Domain . . . 12
- 3.5 Task 5: Migrate On-premises User Accounts to the Custom Domain . . . 15

4 End of Lab 9 **17**
- 4.1 demo: title: 'Demo: Deploying an ARM Template' module: 'Module 1: Exploring Azure Resource Manager' . . . 17

5 Demo: Deploying an ARM Template **17**
- 5.1 Instructions . . . 17

6 Module 1 – Lab 1 – Lab Introduction **18**
- 6.1 Exercise 1 - Create Connectors . . . 18
  - 6.1.1 Task 1 - Obtain Your Microsoft 365 Credentials . . . 19
  - 6.1.2 Task 2 - Create a Custom Receive Connector . . . 19
  - 6.1.3 Task 3 - Create a Custom Send Connector . . . 21

7 End of Lab 1 **21**

8 Module 2 – Lab 2 - Exercise 1 – Create Mail Flow Rules **21**
- 8.1 Task 1 - Create Mail Flow rule for sensitive material . . . 22
- 8.2 Task 2 - Create first Mail Flow rule for attachments . . . 23
- 8.3 Task 3 - Create second Mail Flow rule for attachments . . . 25
- 8.4 Task 4 – Create Mail Flow rule restricting email size . . . 25

9 End of Lab 2 **26**

10 Module 3 – Lab 3 - Exercise 1 - Create Hygiene Filters **26**
- 10.1 Task 1 - Create a Malware Filter . . . 27
- 10.2 Task 2 - Create a Connection Filter . . . 28
- 10.3 Task 3 - Create a Spam Filter . . . 28

11 End of Lab 3 **30**

12 Module 4 - Lab 4 - Exercise 1 – Managing Messaging Compliance **30**
- 12.1 Task 1: Prepare for eDiscovery . . . 30
- 12.2 Task 2: Creating a Custom DLP policy . . . 31
- 12.3 Task 3: Confirming the Status of the Custom DLP policy . . . 33

12.4 Task 4: Performing a Message Trace . . . 34
12.5 Task 5: Reviewing Active MRM Policies with PowerShell . . . 36
12.6 Task 6: Creating a Retention Label . . . 37
12.7 Task 7: Creating a Retention Label Policy . . . 38
12.8 Task 8: Creating an eDiscovery Case . . . 39

13 End of Lab 4 **41**

14 Module 6 – Lab 5 - Exercise 1 - Implement ActiveSync **41**
14.1 Task 1 - Create Recipient mailboxes . . . 41
14.2 Task 2 - Maintain ActiveSync For a Single Mailbox . . . 42
14.3 Task 3 - Maintain ActiveSync For a Multiple Mailboxes . . . 42

15 End of Lab 5 **43**

16 Module 7 - Lab 6 - Exercise 1 - Manage Roles and Permission Policies **43**
16.1 Task 1 - Create an Admin Role . . . 43
16.2 Task 2 - Manage an Admin Role . . . 44
16.3 Task 3 -Create an Outlook Web App Policy . . . 45
16.4 Task 4: Assign an Outlook Web App Policy to a user mailbox . . . 45

17 End of Lab 6 **46**

18 Module 8 – Lab 7 - Exercise 1 – Create Exchange Recipients **46**
18.1 Task 1 - Create a Cloud Recipient . . . 46

19 Proceed to Lab 7 - Exercise 2 **48**

20 Module 8 - Lab 7 - Exercise 2 - Create Groups **48**
20.1 Task 1 - Create an On-premises Distribution Group . . . 48
20.2 Task 2 - Create a Cloud Distribution Group . . . 49
20.3 Task 3 - Create a Microsoft 365 Group . . . 50

21 End of Lab 7 **52**

22 Module 9 - Lab 8 - Exercise 1 - Create Public Folders **52**
22.1 Task 1 - Create a Public Folder Mailbox . . . 52
22.2 Task 2 - Create a Public Folder . . . 52

23 Proceed to Lab 8 - Exercise 2 **53**

24 Module 9 - Lab 8 - Exercise 2 - Manage Public Folders **53**
24.1 Task 1 - Manage Public Folder Mail Settings . . . 53
24.2 Task 2 - Manage Public Folder Settings . . . 53
24.3 Task 3 - Manage Public Folder Permissions . . . 54

25 End of Lab 8 **54**

26 Module 10 - Lab 9 - Exercise 1 - Prepare Azure AD for Hybrid Synchronization **54**
26.1 Task 1: Configure your tenant to support local mail transport . . . 55
26.2 Task 2: Create a Custom Domain in Microsoft 365 . . . 56
26.3 Task 3: Configure the UPN name for custom domain . . . 61
26.4 Task 4: Enable Exchange for the Custom Domain . . . 62
26.5 Task 5: Migrate On-premises User Accounts to the Custom Domain . . . 65

27 End of Lab 9 **68**

28 Module 12 - Lab 10 - Exercise 1 - Configure Your Hybrid Deployment **68**
28.1 Task 1: Create Adatum's Hybrid Exchange deployment . . . 68
28.2 Task 2: Configure Mail Flow Settings . . . 71
28.3 Task 3: Prepare for testing by creating on-premises user mailboxes . . . 72
28.4 Task 4: Create a new Outbound Connector . . . 73

29 Proceed to Lab 10 - Exercise 2 **76**

30 Module 12 - Lab 10 - Exercise 2 - Test your Hybrid Deployment **76**
30.1 Task 1: Test the Hybrid topology 76
30.2 Task 2: Migrate an on-premises mailbox to test your connectors 79
30.3 Task 3: Test the newly migrated mailbox 80

31 Module 12 - Lab 10 - Exercise 3 – Final Assessment **82**

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-203T00-Microsoft-365-Messaging/{{ 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-203T00-Microsoft-365-Messaging/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

3 Module 10 - Lab 9 - Exercise 1 - Prepare Azure AD for Hybrid Synchronization

In this lab you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Adatum has decided to transition from their current Microsoft Exchange on-premises deployment to a hybrid deployment that utilizes Exchange Online within Microsoft 365. Adatum's CTO has tasked you with implementing this hybrid deployment. In this lab, you will perform the tasks necessary to prepare your messaging environment for your eventual hybrid deployment.

To complete this task, you must first prepare Azure Active Directory to support the hybrid synchronization between Exchange on-premises and Exchange Online. This will require that you:

- Configure your lab environment to support local mail transport
- Add an accepted domain to your Azure AD forest
- Configure the UPN Name for the new domain
- Configure Exchange to use the new domain
- Enable directory synchronization by installing and running the Microsoft Azure Active Directory Connect tool
- Perform a Full Synchronization to migrate Adatum's on-premises user accounts to the new domain in Microsoft 365

While your trial tenant has already been set up by your lab hosting provider, you must ensure that your local, on-premises Active Directory is ready for hybrid synchronization before you create your hybrid deployment. You will do this by adding a custom, accepted domain to the Azure Active Directory forest and then configure Exchange to use the new accepted domain.

Once you finish configuring Azure AD for hybrid synchronization in this lab, you will then set up Exchange for a hybrid deployment and then test your new deployment.

3.1 Task 1: Configure your tenant to support local mail transport

Before you begin setting up Adatum's hybrid deployment, you must first configure your hosted lab environment to support local mail transport.

IMPORTANT: The steps that you perform in this task are NOT required to set up a hybrid environment in a real-world scenario. Instead, they must be performed to configure the hosted virtual machines used in this training lab so that email can be sent locally between on-premises and cloud users when testing your hybrid deployment.

1. Switch to LON-EX1 and if necessary, log in as the **Administrator** account with a password of **Pa55w.rd**.
2. If your Edge browser is still open from Lab 1, then minimize the browser now (do not close it).
3. You need to open the **Network and Sharing Center**. To do so, select the network icon on the right-side of the system tray at the bottom of the screen (which displays **Adatum.com Internet access**), and in the menu that appears, select **Network & Internet settings**.
4. In the **Settings** window, scroll to the bottom of the **Status** pane on the right and select **Network and Sharing Center**.
5. In the **Network and Sharing Center**, under the **View your active networks** group, select **Ethernet** (which appears to the right of **Connections**:).
6. In the **Ethernet Status** window, select the **Properties** button that appears at the bottom of the window.
7. In the **Ethernet Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** and then select the **Properties** button.

   WARNING: Do NOT select the check box for **Internet Protocol Version 4 (TCP/IPv4)**, which will uncheck it. This check box MUST remain checked. Simply select this item to highlight it so that you can update its properties.
8. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window is already set up to use an existing IP address. Since you are going to add an additional IP address, select the **Advanced** button in the bottom-right corner of the screen.
9. In the **Advanced TCP/IP Settings** window, in the **IP Settings** tab, it displays two groups: **IP addresses** and **Default gateways**.

   Under the **IP addresses** group, select the **Add...** button.
10. A **TCP/IP Address** pop-up window is displayed. Enter **10.0.0.6** in the **IP address** field, enter **255.255.255.0** in the **Subnet mask** field, and then select **Add**.

    NOTE: If you enter the IP address or subnet mask incorrectly, you will receive an error when selecting **Add**. If this occurs, you must close the window and then reopen it before entering the correct values. If you do not close the window and reopen it, you will still receive the error even if you enter the values correctly.
11. In the **Advanced TCP/IP Settings** window, it should now display **10.0.0.6** as a supported IP address, with a subnet mask of **255.255.255.0**. Select **OK**.
12. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, select **OK**.
13. In the **Ethernet Properties** window, select **Close**.
14. In the **Ethernet Status** window, select **Close**.
15. Close the **Network and Sharing Center** window.
16. Close the **Settings** window.

3.2 Task 2: Create a Custom Domain in Microsoft 365

Not every company has just one domain; in fact, many companies have more than one domain. Adatum has just purchased a new domain (xxxUPNxxx.xxxCustomDomainxxx.xxx; the exact name of which is provided

by your lab hosting provider) that resides in Microsoft Azure but not in Adatum's on-premises environment. To support Adatum's new custom domain, your lab hosting provider took on the role of Adatum's third-party domain registrar.

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

Most companies do not personally manage their domains' DNS records themselves; instead, they have a third-party resource that manages these records for them. To assist in this effort, Microsoft 365 provides certain third-party domain registrars with an automation tool that automatically adds and replaces a company's DNS records. The automation tool also federates the sign in credentials for the third-party registrars and Microsoft 365. Using a tool to automatically maintain DNS records is a much-welcomed improvement from the days when companies had to manually maintain these records, which oftentimes introduced human error into a rather complicated process. Because these tools eliminate the need to manually add the DNS records, they eliminate human error from the process.

That being said, for the purpose of this lab, you will be asked to manually create the necessary DNS records required by this new custom domain. In the other Microsoft 365 training courses that use a custom domain (such as MS-101T00 and MS-030T00), the custom domain and its DNS records will be added into Adatum's Microsoft 365 deployment by the lab hosting provider, who will take on the role of the third-party domain registrar for Adatum. However, this MS-203T00 training course will task you with adding the domain and creating its required DNS records so that you gain experience and understanding of what the DNS records are about and why they are required for a new domain.

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

1. Switch to **LON-DC1** and, if necessary, log in as **Administrator** and password **Pa55w.rd**.
2. You must now open **Windows PowerShell**. Select the magnifying glass (Search) icon on the taskbar at the bottom of the screen and type **powershell** in the Search box that appears.

   In the list of search results, right-click on **Windows PowerShell** (do not select Windows PowerShell ISE) and select **Run as administrator** in the drop-down menu that appears. Maximize your PowerShell window.
3. At the command prompt, you should run the following command to create a new zone in your on-premises DNS:

   IMPORTANT: Before you run the following command, remember to replace **xxxUPNxxx** with the unique UPN name assigned to your tenant by your lab hosting provider, and replace **xxxCustomDomainxxx.xxx** with your lab hosting provider's custom domain name:

   ```
   dnscmd /zoneadd xxxUPNxxx.xxxCustomDomainxxx.xxx /DsPrimary
   ```
4. Minimize your Windows PowerShell window (do NOT close it as you will use it later).
5. You will now access the **Microsoft 365 admin center** from LON-DC1. Select the **Microsoft Edge** icon on your taskbar and enter the following URL in the address bar: **https://portal.office.com.**
6. On the **Sign in** page, enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), and then enter the tenant email password provided by your lab hosting provider on the **Enter password** page. Select **Sign in.**
7. On the **Stay signed in?** window, select the **Don't show this again** check box and then select **Yes.**
8. If a **Get your work done with Office 365** window appears, select the **X** in the upper right-hand corner to close it.
9. In the **Office 365 home** page, in the column of Microsoft 365 app icons on the left-side of the screen, select the **Admin** icon to navigate to the **Microsoft 365 admin center**.

10. In the **Microsoft 365 admin center**, in the left-hand navigation bar, select **Show all,** select **Settings**, and then under the **Settings** group select **Domains**.

11. On the **Domains** page, note that in the list of domains, only the **xxxxxZZZZZZ.onmicrosoft.com** domain appears. The existing on-premises **adatum.com** domain does not appear in the list of Microsoft 365 domains.

    To add Adatum's new Microsoft 365 domain, select **+Add domain** in the menu bar that appears above the list of domains; this will start the **Add domain** wizard.

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

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

14. On the **Verify you own this domain** page, you must copy the **TXT value** (NOT the TXT name) so that you can configure the domain later on in DNS Manager.

    To do so, select the **Copy record** icon that appears to the left of the **TXT value** (to the left of **MS=msXXXXXXXX**). If a dialog box appears, select **Allow access** to copy this value from the webpage to your clipboard.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Exchange and Exchange Online Protection is displayed by default and its check box is also selected by default. To see the other two services, select **Advanced Options**. Note that under **Advanced Options**, neither the **Skype for Business** nor the **Intune and Mobile Device Management for Microsoft 365** check boxes are selected.

    This is sufficient for Adatum; you should NOT select either of these two check boxes. Only the **Exchange and Exchange Online Protection** check box should be selected.

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

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

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

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

    - In the **MX Records** section, under the **Points to address or value** column, select the copy icon that appears to the left of the expected value (for example, **xxxUPNxxx-xxxCustomDomainxxx-xxx.mail.protection.outlook.com**) to copy this value to the clipboard. If a dialog box appears, select **Allow access** to allow the webpage to copy the value to the clipboard.
    - You must now switch to DNS Manager. On the taskbar at the bottom of the page, select the **DNS Manager** icon.
    - In **DNS Manager**, under **Forward Lookup Zones**, the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain should be selected from when you earlier left off. If not, select this zone now. You should

see the **TXT** record that you created earlier. You must now create a **Mail Exchanger (MX)** record for this domain.

Under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Mail Exchanger (MX)...**

- In the **New Resource Record** window, in the **Mail Exchanger (MX)** tab, leave the **Host or child domain** field blank, but right-click in the **Fully qualified domain name (FQDN) of mail server** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you copied to the clipboard in **step a** above.
- Select **OK**. Note how this Mail Exchanger (MX) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.
- Switch back to the **Add DNS records** page in the Microsoft 365 admin center by selecting the **Microsoft Edge** icon on the taskbar at the bottom of the page. At this point, you can either select **Continue** at the bottom of the **Add DNS records** page to verify the MX record that you just added, or you can wait until you have added all three records and then select **Continue** to verify all three records at once.

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

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

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

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

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

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

    - On the taskbar at the bottom of the page, select the **DNS Manager** icon.
    - In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Alias (CNAME)...**
    - In the **New Resource Record** window, enter **autodiscover** in the **Alias name (uses parent domain if left blank)** field.
    - Right-click in the **Fully qualified domain name (FQDN) for target host** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you earlier copied to the clipboard.
    - Select **OK**. Note how this Alias (CNAME) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.

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

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

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

    - On the **Add DNS records** page, in the **TXT Records** section, under the **TXT value** column, select the copy icon that appears to the left of the expected value (for example, **v=spf1 include:spf.protection.outlook.com -all**) to copy this value to the clipboard.
    - On the taskbar at the bottom of the page, select the **DNS Manager** icon.
    - In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **Other New Records...**
    - In the **Resource Record Type** window that appears, in the **Select a resource record type** field, scroll down and select **Text (TXT),** and then select the **Create Record...** button at the bottom of the window.
    - In the **New Resource Record** window, in the **Text (TXT)** tab, leave the **Record name** field blank. However, right-click in the **Text** field and select **Paste** from the menu that appears. This will paste in the expected **TXT value** that you earlier copied to the clipboard.
    - Select **OK**.
    - On the **Resource Record Type** window, select **Done**.

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

    Minimize the DNS Manager window.

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

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

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

32. Once the domain setup process is complete and the three DNS records validated successfully for the **Exchange and Exchange Online Protection** service, the **Domains** page will be displayed. Verify the **Domain status** for your new domain is **Healthy**.

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

3.3 Task 3: Configure the UPN name for custom domain

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

If you recall, your VM environment was created by your lab hosting provider with an on-premises domain titled **adatum.com**. This domain included several on-premises user accounts, such as Holly Spencer, Laura Atkins, and so on. Then in the prior task, you created a custom, accepted domain for Adatum titled **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx was the unique UPN name assigned to your tenant, and xxxCustomDomainxxx.xxx was the name of your lab hosting provider's custom domain).

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

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

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

1. You should still be logged into LON-DC1 as the **Administrator** with a password of **Pa55w.rd**; if necessary, log in now.
2. In this task, you will run two PowerShell commands. To save you from having to type in the commands (which are quite lengthy), you will copy the commands from these instructions and then paste them into Notepad. You will then replace the custom domain name placeholder in the commands with the actual domain name, and then you will copy and paste each command from Notepad into PowerShell.

   Select the **magnifying glass (Search)** icon on the taskbar and then enter **note** in the Search field. In the menu that appears, select **Notepad**. Maximize the Notepad window once it opens.
3. While the PowerShell commands that you need to run are provided in steps 7 and 8, it will be easier to copy these steps into Notepad, perform a **Replace** command to replace the custom domain name parameter with your actual new domain name, and then copy the commands in Notepad and paste them into PowerShell. This will save you from having to enter some lengthy PowerShell commands.

   Therefore, copy the PowerShell commands from **steps 7 and 8** below and paste them into Notepad (**Hint:** to make it easy, copy all the text for steps 7 and 8 and not just the PowerShell commands; that way you can do one Copy statement rather than 2 Copy statements of just the PowerShell commands).
4. Once you have copied steps 7 and 8 into Notepad, select **Edit** on the Notepad menu bar and then select **Replace**.
5. In the **Replace** window, copy **xxxUPNxxx.xxxCustomDomainxxx.xxx** and paste it into the **Find what** field. In the **Replace with** field, enter the new domain you previously added, select **Replace all**, and then close the **Replace** window.

   Important: Review the Notepad document and verify that both commands were updated by replacing **xxxUPNxxx.xxxCustomDomainxxx.xxx** with the new accepted domain name. Verify you spelled the new domain name correctly.
6. If **Windows PowerShell** is still open, then select the **Windows PowerShell** icon on your taskbar; otherwise, you must open and elevated instance of **Windows PowerShell** just as you did earlier (remember to **Run as administrator)**.
7. You will now begin the process of copying each of the PowerShell commands (from this step through step 8) from Notepad and pasting and running them in Windows PowerShell.

In the following PowerShell command, the **Set-ADForest** cmdlet modifies the properties of an Active Directory forest, and the **-identity** parameter specifies the Active Directory forest to modify.

Select the **Notepad** icon on the taskbar and then copy the following command from Notepad (select the command, right-click on it, and then select **Copy**), paste it into PowerShell at the command prompt (right click on the command prompt and select **Paste).**

Note: Traditionally, you must right-click at the command prompt, select Paste, and then hit ENTER on the keyboard to run a command. However, in some VM environments, you just have to right-click at the command prompt to both paste in the copied command AND run it.

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

8. Copy the following command from Notepad, paste it into PowerShell at the command prompt, and then run it.

   This command changes all existing adatum.com accounts to the new UPN @xxxUPNxxx.xxxCustomDomainxxx.xxx domain:

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

9. Wait for PowerShell to complete the prior command and return to the command prompt, and then close the Windows PowerShell window.
10. Close Notepad (do not save the untitled document).
11. Leave the Edge browser and all tabs open and proceed to the next task.

3.4 Task 4: Enable Exchange for the Custom Domain

In this task, you will log into the on-premises Exchange Server (LON-EX1) VM and enable your Exchange on-premises environment for the accepted domain (**xxxUPNxxx.xxxCustomDomainxxx.xxx**) that you added and configured in the prior tasks. You will run a series of PowerShell commands in the Exchange Management Shell, and you will update additional settings in the on-premises Exchange Admin Center.

1. Switch to **LON-EX1** and, if necessary, log in as the **Administrator** with a password of **Pa55w.rd**. If you had to log in and the **Server Manager** application automatically opened, then close it now.
2. In this task, you will enter a series of Exchange-specific PowerShell commands through the **Exchange Management Shell**. These commands will enable your on-premises Exchange environment for the new **xxxUPNxxx.xxxCustomDomainxxx.xxx** accepted domain.

   To expedite running these commands, open **Notepad just as you did in the prior task**, maximize the Notepad window, and then copy **steps 5-15** below and paste them into the Notepad document (to make it easy, copy all the text for steps 5-15 and not just the PowerShell commands; that way you can do one Copy statement rather than 11 Copy statements of just the PowerShell commands).

   Warning: Some lab hosting providers' VM environments limits the amount of text that can be copy and pasted at one time into a VM. If this occurs within your VM environment, you may have to copy and paste steps 5-15 in chunks to get all 11 steps copied into Notepad.

3. In the prior task, after you copied the two steps into Notepad, you did one mass replace on xxxUPNxxx.xxxCustomDomainxxx.xxx. However, in this task, one of the commands just references xxxCustomDomainxxx.xxx and not the xxxUPNxxx UPN name, so in this task, you should replace each portion of the domain name separately.

   After copying the commands from steps 5-15 into Notepad, perform the following two (2) **Replace** commands in Notepad:

   - Replace all instances of **xxxUPNxxx** with the **UPN Name** provided by your lab hosting provider.
   - Replace all instances of **xxxCustomDomainxxx.xxx** with the accepted domain provided by your lab hosting provider.

- **Important:** Review the Notepad document and verify that all instances of xxxUPNxxx have been replaced with your UPN Name, and all instances of xxxCustomDomainxxxx.xxx have been replaced with your new domain name.
- Close the **Replace** window.

4. To open the **Exchange Management Shell**, select the Windows icon on the bottom left corner of the taskbar, and then in the menu select **Microsoft Exchange Server 2019** to expand this program group, and then in the group, select **Exchange Management Shell**.

   Maximize the **Exchange Management Shell** window once it opens. Wait for the command prompt to appear before proceeding.

5. You will now begin the process of copying each of the PowerShell commands in Notepad and then pasting and running them in the Exchange Management Shell.

   Select the **Notepad** icon on the taskbar, and in your Notepad document, start with this Step 5.

   Select the following PowerShell command from step 5 in the Notepad document, right-click on it, and select **Copy**, paste it into the Exchange Management Shell at the command prompt (right click on the command prompt and select **Paste;** Note – in some VM environments, just right-clicking at the command prompt will paste in the copied command), and then press Enter on your keyboard.

   This command will add a new send connector with a wildcard (asterisk) to accept all emails from any domain:

   New-SendConnector -Name ”To Internet” -AddressSpaces ”*”

6. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will add the accepted xxxUPNxxx.xxxCustomDomainxxx.xxx domain as a Micro, set it as a trusted domain, and assign it the Alias of A.Datum:

   New-AcceptedDomain -DomainName ”xxxUPNxxx.xxxCustomDomainxxx.xxx” -DomainType Authoritative -Name ”A.Datum”

7. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the default email policy for every user to have its primary email address as the accepted domain of xxxUPNxxx.xxxCustomDomainxxx.xxx:

   Set-EmailAddressPolicy -Identity ”Default Policy” -EnabledPrimarySMTPAddressTemplate ”SMTP:%m@xxxUPNxxx.xxxCustomDomainxxx.xxx”

8. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will update the default email policy that was just changed in the previous command:

   Update-EmailAddressPolicy -Identity ”Default Policy”

9. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the OWA Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OWA:

   Set-OwaVirtualDirectory -Identity ”LON-EX1\OWA (Default Web Site)” -ExternalUrl https://xxxUPNxxx.xxxCustom -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OWA

   NOTE: Ignore the warning that’s displayed. This warning is addressed when you run the next command.

10. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the ECP Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ECP:

    Set-EcpVirtualDirectory -Identity ”LON-EX1\ECP (Default Web Site)” -ExternalUrl https://xxxUPNxxx.xxxCustomI -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ECP

11. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Active Sync Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync:

Set-ActivesyncVirtualDirectory -Identity "LON-EX1\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync

12. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Web Services Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ews/exchange.asmx:

    Set-WebServicesVirtualDirectory -Identity "LON-EX1\EWS (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ews/exchange.asmx -InternalUrl https://xxxUPNxxx.xxxCustomDom

    NOTE: For this **Set-WebServicesVirtualDirectory** command, if you receive a prompt that indicates the InternalURL parameter can't be resolved, enter **A** for **Yes to All** to continue and then press **Enter**.

13. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the OAB Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx /OAB:

    Set-OabVirtualDirectory -Identity "LON-EX1\OAB (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustom -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OAB

14. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Outlook Anywhere external host name to xxxUPNxxx.xxxCustomDomainxxx.xxx and to set the authentication method to NTLM and to require external clients to use SSL to make the connection:

    Set-OutlookAnywhere -Identity "LON-EX1\Rpc (Default Web Site)" -ExternalHostname xxxUPNxxx.xxxCustomDomainxxx.xxx -ExternalClientsRequireSsl $true -ExternalClientAuthenticationMethod NTLM -InternalHostname xxxUPNxxx.xxxCustomDomainxxx.xxx -InternalClientsRequireSsl $true -InternalClientAuthenticationMethod NTLM

15. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the Outlook certificate to *.xxxCustomDomainxxx.xxx:

    Set-OutlookProvider EXPR -CertPrincipalName:*.xxxCustomDomainxxx.xxx

16. Close your Exchange Management Shell window by selecting the **X** in the upper-right hand corner.
17. Close Notepad (do not save the untitled document).
18. To enable Exchange for the custom domain, you must identify the Exchange services that you want to assign to the *.xxxCustomDomainxxx.xxx certificate.

    If you have a tab open in your Edge browser for the on-premises **Exchange admin center,** then proceed to the next step; otherwise, select the **Windows** icon on the taskbar, select the **Microsoft Exchange Server 2019** group, and then select **Exchange Administrative Center.**

    Note: If you receive a page indicating **Your connection isn't private**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select the **Advanced** button, and then select **Continue to localhost (unsafe)**.

19. In the **Exchange Admin Center**, log in as **adatum\Administrator** with a password of **Pa55w.rd**.
20. In the **Exchange admin center**, select **servers** in the left-hand navigation pane.
21. On the **servers** page, the **servers** tab is displayed by default in the list of tabs across the top of the page. Select the **certificates** tab.
22. In the list of certificates, select the **wildcard_xxxCustomDomainxxx_xxx** certificate (where xxxCustomDomainxxx_xxx is the name of you accepted domain) and then select the **pencil (Edit)** icon on the menu bar.
23. In the **wildcard_xxxCustomDomainxxx_xxx** window, select **services** in the left-hand pane.
24. In the list of services, select the **SMTP** check box and the **IIS** check box, and then select **Save**. Select **Yes** in the **Warning** dialog box that appears.
25. In the **Exchange admin center**, select **mail flow** in the left-hand navigation pane and then select the **accepted domains** tab at the top of the page.

26. In the list of accepted domains, you must set the **A.Datum** domain (where the **Accepted Domain** is xxxUPNxxx.xxxCustomDomainxxx.xxx) as the Default domain. Select this domain (if it's not already selected by default), then select the **pencil (Edit)** icon on the menu bar above the list of domains.
27. In the **A.Datum** window, under the **This accepted domain is** setting, verify the **Authoritative** option is selected (this should have been set to Authoritative in the step 6 PowerShell command). Then select the **Make this the default domain** check box and select **Save**.

    In the list of domains, the **A.Datum** domain should now be listed as the **default domain** and the **Domain Type** should be **Authoritative**.
28. Close the Edge browser so that you close the Exchange admin center and proceed to the next task.

3.5 Task 5: Migrate On-premises User Accounts to the Custom Domain

In this lab, you will log into the Domain Controller (LON-DC1) VM and enable directory synchronization. To do this, you must first download the setup wizard for the Microsoft Azure Active Directory Connect tool. You will then run the installation wizard to enable and configure directory synchronization. This will perform a full synchronization that migrates all of Adatum's on-premises user accounts to the new accepted domain in Microsoft 365.

1. Switch to **LON-DC1** and, if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your Edge browser session, the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab should still be open; if not, then navigate to them now.

   Select the **Microsoft 365 admin center** tab, which should be displaying the **Domains** page.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users**, and then select **Active users**.
4. You are now going to navigate to the **Microsoft Download Center** to download the **Azure AD Connect** tool.

   In the **Active users** window, on the menu bar, select the **ellipsis (More actions)** icon, and then in the drop-down menu that appears, select **Directory synchronization**.

   Note: If the **ellipsis (...)** icon does not appear on the menu bar, then at the very top of the left-hand navigation pane, select the **Navigation menu (three vertical lines)** icon to minimize the navigation pane, which removes the text. This expands the size of the **Active users** page, so the ellipsis icon should now appear on the menu bar. If for some reason you cannot locate the **Directory synchronization** option, then you can navigate directly to the **Azure AD Connect** page in the **Microsoft Download Center** by opening a new tab in your Edge browser and entering the following URL in the address bar (if you navigate directly to this URL, you can skip the next step): **https://www.microsoft.com/en-us/download/details.aspx?id=47594**[](https://www.microsoft.com/en-us/download/details.aspx?id=47594)
5. In the **Azure Active Directory preparation** window, select **Go to the Download center to get the Azure AD Connect tool**. This opens a new tab in your browser and takes you to the Microsoft Download Center.
6. In the **Microsoft Download Center**, scroll down to the **Microsoft Azure Active Directory Connect** section and select the **Download** button.
7. Once the download is complete, in the notification bar at the bottom of the page, select **Open file** that appears below the **AzureADConnect.msi** file.
8. This initiates the installation of the **Microsoft Azure Active Directory Connect Tool**.

   Note: After the wizard begins, the **Microsoft Azure AD Connect Tool** window may disappear. If this occurs, find the icon for it on the task bar and select it.

   On the **Welcome to Azure AD Connect** window in the setup wizard, select the **I agree to the license terms and privacy notice** check box and then select **Continue**.
9. On the **Express Settings** page, read the instruction regarding a single Windows Server AD forest (which is the scenario in your VM lab environment) and then select **Use express settings**.

10. On the **Connect to Azure AD** window, you must enter the user credentials for a Microsoft 365 user account that has been assigned the Microsoft 365 Global Administrator role. Enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **USERNAME** field, enter (or copy and paste) the tenant email password provided by your lab hosting provider in the **PASSWORD** field, and then select **Next.**

    Note: You may have to tab out of the **PASSWORD** field to enable the **Next** button.

11. On the **Connect to AD DS** page, enter **adatum\Administrator** in the **USERNAME** field, enter **Pa55w.rd** in the **PASSWORD** field, and then select **Next.**

    Note: You may have to tab out of the **PASSWORD** field to enable the **Next** button.

12. In the **Azure AD sign-in configuration** window, select the **Continue without matching all UPN suffixes to verified domains** check box at the bottom of the page and then select **Next**.

13. On the **Ready to configure** screen, select the **Start the synchronization process when configuration completes** check box (if it's not already selected), and select the **Exchange hybrid deployment** check box since you are preparing Azure AD Connect for an Exchange hybrid deployment.

    Select **Install**.

14. The installation will usually take 5 to 10 minutes to complete. On the **Configuration complete** window, verify you receive a message at the top of the window indicating **Azure AD Connect configuration succeeded.** Ignore the warning indicating the Active Directory Recycle Bin is not enabled for your forest. This recycle bin will not be needed for the purposes of this VM lab environment.

    Select **Exit**.

15. In the taskbar at the bottom of the screen, select the **magnifying glass (Search)** icon, and then in the Search box, enter **sync**. In the menu that appears, select the **Synchronization Service** desktop application to open it.

16. Maximize the **Synchronization Service Manager** window.

17. In the **Synchronization Service Manager** window, on the ribbon at the top of the page, the **Operations** tab is displayed by default so that you can monitor the synchronization process.

18. Wait for the **Export** profile to complete for **xxxxxZZZZZZ.onmicrosoft.com** (the second task in the list); when it finishes, its **Status** should be **completed-export-errors**.

    Once this status appears, select this row.

19. In the bottom portion of the screen, a detail pane appears showing the detailed information for this operation that you just selected.

    - In the **Export Statistics** section, note the number of users that were added and the number that were updated.
    - In the **Export Errors** section on the right, note the two errors that appear. Select the link for the first error that appears under the **Export Errors** column.

      The first error is an "add user"" error for user **Ngoc Bich Tran**. Review the error and then close the window. Select the link for the second error, which is an "add user" error for user **An Dung Dao**. Review this error and then close the window.

      These are users whose on-premises accounts have an invalid UPN, which in turn caused UPN validation errors during the synchronization process; therefore, these users were not synchronized by the Azure AD Connect tool.

      Note: Because a synchronization had not been performed prior to this, the initial synchronization was a **Full Synchronization** (see the **Profile Name** column in the **Connector Operations** pane at the top of the page). Because the synchronization process will continue to run automatically every 30 minutes, any subsequent synchronizations will display **Delta Synchronization** as its **Profile Name**. If you leave the **Synchronization Service Manager** window open, after 30 minutes you will see that it attempts to synchronize the two users who were not synchronized during the initial synchronization. These will display as a **Delta Synchronization**.

20. Close the **Synchronization Service Manager**.

21. In your Edge browser, close the **Download Microsoft Azure AD Connect** tab, and then in the **Microsoft 365 admin center** tab, close the **Azure Active Directory preparation** pane. This will return you to the **Active users** list.

    Note: If you had to select the **Navigation menu** icon at the very top of the left-hand navigation pane in the earlier step to see the ellipsis icon, then select this **Navigation menu** icon again to expand the pane and display the text associated with each icon. Seeing the text associated with each icon makes it easier to navigate through the admin center.

22. On the **Active users** page, note that all the existing Microsoft 365 user accounts are the predefined users that were created in your tenant by your lab hosting provider. Select the **Refresh** icon on the menu bar to see all the on-premises user accounts that were migrated to the new accepted domain in Microsoft 365.

    Note the **Username** for each of these accounts, which should be in the format of **<alias>@xxxUPNxxx.xxxCusto**
    Also note that each of these user accounts is **Unlicensed**; this indicates that while the on-premises accounts have been migrated to the new domain in Microsoft 365, they have not been assigned an Office 365 license.

    If you scroll down through the list of **Active users**, note that you will see both unlicensed and licensed users; the licensed users are the original list of Microsoft 365 user accounts created by your lab hosting provider.

23. On the right-side of the menu bar at the top of the page, select **Filter**. In the menu that appears, select **Licensed users**. This will display only those user accounts that were all assigned an Office 365 license (these are the Microsoft 365 user accounts that were created by your lab hosting provider).

    In the **Username** column, note how these user accounts were assigned to the **xxxxxZZZZZZ.onmicrosoft.com** domain when they were created by your lab hosting provider.

24. Note how the **Filter** option on the menu bar now displays **Licensed users**. Select **Licensed users** and in the menu that appears, select **Unlicensed users**. This will display all the user accounts that were just migrated from the on-premises **adatum.com** domain to the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain. The migration process did not assign a license to any of these new Microsoft 365 accounts that were just created. If you scroll down through this list, you should not see any of the licensed user accounts in the **xxxxxZZZZZZ.onmicrosoft.com** domain.

    In the **Username** column, note how these user accounts were assigned to the **xxxUPNxxx.xxxCustomDomainxxx.x**
    domain that you earlier created in Microsoft 365.

25. The **Filter** option on the menu bar should now display **Unlicensed users**. Select **Unlicensed users** and in the menu that appears, select **All users**. This will return you to the list of all active user accounts in both the **xxxUPNxxx.xxxCustomDomainxxx.xxx** and **xxxxxZZZZZZ.onmicrosoft.com** domains.

    Congratulations! You have just verified that the Full Synchronization process migrated Adatum's on-premises user accounts to the new accepted domain.

26. Leave your Edge browser and all tabs open as it will be used in the next lab.

4 End of Lab 9

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

5 Demo: Deploying an ARM Template

5.1 Instructions

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

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

   ```
   Sed at malesuada orci, eu volutpat ex
   ```
5. In ac odio vulputate, faucibus lorem at, sagittis felis.
6. Fusce tincidunt sapien nec dolor congue facilisis lacinia quis urna.

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

6 Module 1 – Lab 1 – Lab Introduction

Adatum Corporation runs their legacy applications (such as Microsoft Exchange Server 2019) in an on-premises deployment. However, they recently subscribed to Microsoft 365, thereby creating a hybrid deployment in which they must synchronize their on-premises and cloud deployments.

Throughout the labs in this course, you will take on the persona of Holly Dickson, Adatum's Messaging Administrator. You have been tasked with integrating Adatum's on-premises Exchange environment with Microsoft 365 and Exchange Online. Adatum's project team has decided to implement Microsoft 365 in a pilot project that will not only provide them with experience using the product, but also enable them to match their messaging requirements with the Microsoft 365 feature set.

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

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

- Deployed the trial tenant
- Created a default tenant administrator account (known as the MOD Administrator)
- Created 9 additional user accounts
- Created a custom Microsoft 365 domain in Microsoft Azure
- Created the DNS records in Microsoft Azure that are required to support the custom domain and the selected Microsoft 365 services

6.1 Exercise 1 - Create Connectors

As part of her pilot project for Adatum's Exchange deployment, Holly wants to begin by creating custom send and receive connectors in her on-premises Exchange Server using the on-premises Exchange admin center.

Exchange uses connectors on Exchange servers to enable incoming and outgoing mail flow between services in the transport pipeline on the local Exchange server. In this lab you will log into the Exchange Server VM (LON-EX1) and create custom Receive and Send connectors using the on-premises Exchange Admin Center (EAC) for Adatum's Exchange Server 2019 deployment.

As you complete each task, you should leave the EAC open in your browser for the next lab. This will save you from having to open the EAC at the start of each lab.

6.1.1 Task 1 - Obtain Your Microsoft 365 Credentials

Once you launch the lab, a free trial tenant will be automatically created for you to access 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. You will also be assigned a unique network IP address and UPN name for your Microsoft 365 blob. You will also use this UPN name in various tasks throughout the labs for this course.

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

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

- **Tenant prefix.** This tenant prefix is for the Microsoft 365 user accounts that you will use to sign into Microsoft 365 throughout the labs in this course. The domain for each Microsoft 365 user account is in the format of {user alias}@xxxxxZZZZZZ.onmicrosoft.com, where xxxxxZZZZZZ is the tenant prefix. It consists of two parts - your lab hoster's prefix (xxxxx; some hosters use a generic prefix such as M365x, while others use their company initials or some other designation) and the tenant ID (ZZZZZZ; usually a 6 digit number). Record this xxxxxZZZZZZ tenant prefix value for later use. When any of the lab steps direct you to sign into Microsoft 365 as one of the user accounts (such as the MOD Administrator), you must enter the xxxxxZZZZZZ value that you obtained here as the tenant prefix portion of your .onmicrosoft.com domain.
- **Tenant password.** This is the password provided by your lab hosting provider for the tenant admin account.
- **Custom Domain name.** Your lab hosting provider has created a custom domain name for Adatum that you will use when adding a custom domain into Microsoft 365 in a later lab exercise. The domain name is in the format **xxxUPNxxx.xxxCustomDomainxxx.xxx.** You must replace **xxxUPNxxx** with the UPN name provided by your lab hosting provider, and you must replace **xxxCustomDomainxxx.xxx** with the lab hosting provider's domain name. For example, let's assume your lab hosting provider is Fabrikam Inc. If the UPN number it assigns to your tenant is AMPVU3a and its custom domain name is fabrikam.us, then the domain name for your new custom domain would be AMPVU3a.fabrikam.us. Your instructor will provide you with your lab hosting provider's UPN number and custom domain name.
- **Network IP address.** Write down the **IP Address** value (this is the IP Address of your parent domain; for example, 64.64.206.13).

6.1.2 Task 2 - Create a Custom Receive Connector

Adatum has Microsoft Exchange Server 2019 installed on the Exchange Server VM (LON-EX1). In this task, you will use the Exchange admin center for Exchange Server 2019 to create a custom receive connector for Adatum's on-premises Exchange deployment.

1. Switch to the Exchange Server VM (LON-EX1) and log on as Adatum's **Administrator** account with a password of **Pa55w.rd**.
2. After logging in, the **Server Manager** application will automatically open. Select the **X** in the upper-right corner of the screen to close it.
3. Holly wants to create custom connectors using the on-premises **Exchange Admin Center (EAC)**. To do so, select the **Windows** icon in the lower-left corner of the taskbar, and in the Start menu select the **Microsoft Exchange Server 2019** group. In the program group, select **Exchange Administrative Center**.
4. This will open **Microsoft Edge**, which will attempt to access the EAC. Maximize your browser window.

   Edge will display an error page indicating **Your connection isn't private**.

   Select **Advanced**, which displays a message indicating **This server couldn't prove that it's localhost; its security certificate is from LON-EX1. This may be caused by a misconfiguration or an attacker intercepting your connection.** You received this message because a certificate for the EAC

was not included in your VM lab training environment. In a real-world deployment, this certificate would be required.

Select **Continue to localhost (unsafe)**.

5. In the **Exchange Admin Center** log-in page, enter **adatum\Administrator** in the **Domain\user name** field and **Pa55w.rd** in the **Password** field, and then select **sign in**.
6. In the **Exchange admin center**, in the left-hand navigation pane, select **mail flow.**
7. You will begin by creating a custom receive connector. On the menu bar at the top of the **mail flow** page, select **receive connectors**.
8. On the **receive connectors** page, select the **plus (+) sign** icon on the menu bar to add a new receive connector.
9. In the **new receive connector** window that appears, enter **NewReceiveConnector1** in the **Name** field.
10. Under **Role**, select the **Frontend Transport** option.
11. Under **Type,** select the **Internet (For example, to receive internet mail)** option and then select **Next**.
12. This returns a **new receive connector** window in which you can update **Network Adapter Bindings** for the new receive connector. The purpose of this page is to identify the accepted IP addresses and port that are bound to this new receive connector. In other words, this new receive connector will only receive email from the IP address and port identified here before in turn sending it to the Exchange Server.

    Note: In a real-world environment, some companies will create a receive connector that receives email from all IP addresses and a specific port, which in effect forces their email filters to do the heavy lifting of validating email from specific IP addresses for possible threats. Conversely, other companies that may have been hit by known threats will use custom receive connectors to only accept email from specific IP addresses they know are safe.

    When you create a new receive connector, you can select the IP addresses for that connector from the following options:

    - All available IPv4 addresses
    - All available IPv6 addresses
    - A specific IPv4 or IPv6 address

    When creating a new receive connector, this page displays the default combination of **All available IPv4** addresses and **Port 25** .

    Holly has decided use this default setting; therefore, select **Finish** to assign this default combination of IP addresses and port number to the new receive connector.

    IMPORTANT: By selecting **Finish**, you will receive an **Error** message. You were purposely instructed to select **Finish** so that you can see this error, which indicates that the **Default Frontend LON-EX1** receive connector is already configured to accept all available IPv4 addresses (in other words, IP addresses 0.0.0.0 through 255.255.255.255) for Port 25. **Therefore, this new receive connector that you are creating must have a unique combination of IP address and port number that is different from any existing receive connectors.**

    Select **OK** to close the **Error** message.
13. This returns you to the **Network adapter bindings** window. Select the **pencil (edit)** icon on the menu bar to edit the IP address and port number that will be linked to your new receive connector.
14. In the **edit IP address** window, under the **Address** field, select the **Specify an IPv4 address or an IPv6 address** option.
15. After receiving the previous error, Holly met with Adatum's IT Administrator, who has identified **172.16.0.11** as the IP address he wants bound to this new receive connector (for port 25); therefore, enter this value in the **Address** field.

16. Leave the **Port** at **25**, and then select **Save**. Note how the Network adapter binding for this new receive connector now points to this IP address and port number.

    Note: By updating this network adapter binding, all email sent from the Internet and from IP address 172.16.0.11 through port 25 will be received by this new connector, which in turn will send it to Adatum's Exchange Server.

17. Select **Finish**. Your new receive connector should appear in the list of receive connectors.

18. Leave the Exchange Admin Center open in your browser for the next task.

6.1.3 Task 3 - Create a Custom Send Connector

You will now create a custom send connector in Adatum's on-premises Exchange Server (LON-EX1) using the on-premises EAC.

1. You should still be logged into LON-EX1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.

2. In your Edge browser session, the on-premises **Exchange admin center** should still be open; if not, then perform the same steps that you did in the prior task to open it now.

3. In the **Exchange admin center**, you should still be displaying the **receive connectors** tab on the **mail flow** page from the prior task. In the list of tabs at the top of the page, select the **send connectors** tab.

4. On the **send connectors** window, select the **plus (+) sign** icon on the menu bar to add a new send connector.

5. In the **new send connector** window, enter **NewSendConnector1** in the **Name** field.

6. Under **Type,** select the **Internet (For example, to send internet email)** option and then select **Next**.

7. This returns a **new send connector** window in which you can update **Network settings** for the new send connector. Select the **MX record associated with recipient domain** option and then select **Next**.

8. This returns a **new send connector** window in which you can update the connector's **Address space**. Select the **plus (+) sign** to add a new address space record.

9. In the **add domain** window, you must enter the **Full Qualified Domain Name (FQDN)** of the domain associated with Adatum's Microsoft 365 tenant.

    Note: In Task 1 of this exercise, your instructor provided instruction on how to retrieve your tenant email address. Your FQDN is the value to the right of the @ sign in the **Tenant Email** (for example, **xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). Enter your FQDN in the **Full Qualified Domain Name (FQDN)** field.

10. Leave the value of the **Cost** field to **1**, and then select **Save.**

11. Your new **Address space** record for this send connector should now be displayed. Select **Next**.

12. This returns a **new send connector** window in which you can update the **Source server** for the new send connector. Select the **plus (+) sign** to add a new Source server record.

13. In the **Select a Server** window, you want to select your **Mail server**, which in this virtual lab environment is your **LON-EX1** VM. Since the LON-EX1 server is selected by default, select the **add ->** button, and then select **OK**.

14. LON-EX1 should now appear in the Source server list for this new send connector. Select **Finish**.

15. Close the Exchange admin center.

7 End of Lab 1

8 Module 2 – Lab 2 - Exercise 1 – Create Mail Flow Rules

In this lab, you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. In the prior lab, you created new send and receive connectors for Adatum's on-premises Exchange Server 2019 deployment.

Since Adatum has deployed Microsoft 365 and is looking to implement a hybrid Exchange environment, Holly will now begin configuring Exchange Online.

Holly has decided to create a series of mail flow rules designed to protect Adatum's messaging environment. She will do so using her client computer (LON-CL1) to access the Exchange Admin Center for Exchange Online.

In your continuing role as Holly Dickson, you will create mail flow rules for the following scenarios:

- **Sensitive material.** The mail flow rule will quarantine messages sent from inside the organization that have the words "Secret", "Classified", or "Sensitive" in the body or subject of the message.
- **Unscanned attachments.** The mail flow rule will quarantine messages that have attachments that are unscanned. The rule will also generate a reply message that lets the sender know they have sent a message that is undeliverable.
- **Partially scanned attachments.** The mail flow rule will quarantine messages that have attachments that were scanned, but the message scan did not finish. This rule will also generate a reply message that lets the sender know they have sent a message that is undeliverable.
- **Email size.** The mail flow rule will restrict the size of emails.

8.1 Task 1 - Create Mail Flow rule for sensitive material

In this exercise you will access the Exchange Admin Center for Exchange Online using your client PC (LON-CL1). You will then create a mail flow rule that checks for sensitive information in emails sent from inside the organization.

1. Switch to **LON-CL1** and log in as the **Administrator** account with a password of **Pa55w.rd**.
2. Select the **Microsoft Edge** icon either on the desktop or the taskbar. Maximize your browser window when it opens.
3. In your browser navigate to the **Office 365 Home** page by entering the following URL in the address bar: **https://portal.office.com/**
4. In the **Sign in** dialog box, copy and paste in the **Tenant Email** account provided by your lab hosting provider (**admin@xxxxxZZZZZZ.onmicrosoft.com**, where xxxxxZZZZZZ is your unique tenant prefix provided by your lab hosting provider) and then select **Next**.
5. In the **Enter password** dialog box, copy and paste in the **Tenant Password** provided by your lab hosting provider and then select **Sign in**.
6. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
7. If a **Get your work done with Office 365** dialog box appears, select the **X** to close it.
8. In the **Office 365 Home** page, select the **Admin** icon in the column of Microsoft 365 app icons on the left-side of the screen.
9. In the **Microsoft 365 admin center**, in the left-hand navigation bar, select **Show All** to display all the navigation menu options.
10. On the left-hand navigation bar, in the **Admin centers** section, select **Exchange**. This opens the classic Exchange admin center for Exchange Online.

    IMPORTANT: As of this writing, Microsoft is in the process of developing a new Exchange admin center. However, for the purposes of this lab, you will use the classic Exchange admin center because the new Exchange admin center does not yet include the entire Exchange Online feature set. Therefore, while you can select the **New Exchange admin center** option in the left-hand navigation pane to preview the new admin center, you should return to the classic Exchange admin center to complete this lab.
11. In the (classic) **Exchange admin center**, in the left-hand navigation pane, select **mail flow.**
12. At the top of the page, the **rules** tab displays by default. Stay in this tab.
13. The first mail flow rule that you create will check for emails sent from inside the organization that have sensitive words in the email subject line or body. Select the **plus sign (+)** icon in the menu bar, and in the drop-down menu that appears, select **Modify messages.**
14. In the **new rule** window that appears, enter **Sensitive material** in the **Name** field.

15. Note that by default, you can only enter one condition (the **Apply this rule if...** field). Since this rule requires multiple conditions, select **More options...** that appears at the bottom of the window. This displays an **add condition** button that enables you to enter multiple conditions and actions.
16. To add the first condition, select the drop-down arrow in the **Apply this rule if...** field. In the drop-down menu that appears, hover your mouse over **The subject or body...**. In the menu that appears, select **subject or body includes any of these words.**
17. This opens a **specify words or phrases** window. In the text field, enter **secret** and select the **plus (+) sign**.
18. In the text field, enter **classified** and select the plus sign, then repeat this step and enter **sensitive**.
19. The three words should display below the text field. Select **OK**.
20. In the **new rule** window, the three words should display to the right of the **The subject or body includes...** condition. Select the **add condition** button to add another condition.
21. Select the drop-down arrow in the second condition field that appears (Note how this creates a Boolean **And** condition). Hover your mouse over **The sender...** and in the menu that appears, select **is external/internal**.
22. In the **select sender location** window, select the drop-down arrow, select **Inside the organization**, and then select **OK**.
23. Select the drop-down arrow in the **Do the following...** field. Hover your mouse over **Redirect the message to...** and in the menu that appears, select **hosted quarantine.**
24. Select the **add action** button to add another action.
25. Select the drop-down arrow in the second action field that appears. Hover your mouse over **Apply a disclaimer to the message...** and in the menu that appears, select **append a disclaimer.**
26. To the right of the second action field that displays **Append the disclaimer...,** select **Enter text.**
27. In the **specify disclaimer text** window, enter the following message in the field: **This message contains sensitive material that can harm the company or your team.**
28. Select **OK.**
29. To the right of the second action field that displays **Append the disclaimer...,** select **Select one.**
30. In the **specify fallback action** window, **Wrap** displays as the default fallback option. This is the option you want to select as the fallback option (Wrap means if the disclaimer cannot be inserted into the original email, it will attach the message to a new disclaimer email) so select **OK**.
31. Scroll down in the **new rule** window and under the **Properties of this rule** section, verify the **Audit this rule with severity level:** checkbox is selected. If it's not checked, then select it now.
32. Select the severity level drop-down arrow and select **Medium**.
33. In the **Choose a mode for this rule:** option, select **Enforce**.
34. Select **Save.**
35. This returns you to the **rules** tab in the Exchange admin center. The new **Sensitive material** rule should display in the list of rules. This rule should be selected, and a **Sensitive material** pane should appear on the right that displays the conditions and actions of this rule. Verify the conditions and actions are correct; if corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
36. Leave the Exchange Admin Center open to the **rules** tab on the **mail flow** page and proceed to the next task.

8.2 Task 2 - Create first Mail Flow rule for attachments

In this exercise you will create two mail flow rules related to attachments. Adatum wants to check for emails containing attachments that were either not scanned or the scanning did not complete. You cannot include both conditions in one rule, since multiple conditions in a mail flow rule are treated in a Boolean **AND** fashion (for example, condition 1 is True AND condition 2 is True; this is similar to what you did in the prior task where you checked for specific words in the email AND the email was received from inside the organization).

In this case, it does not make logical sense to create just one rule that checks for attachments that were not scanned AND for attachments in which scanning did not complete. Therefore, you will need to create two rules; one for messages with attachments that were not scanned and one for messages with attachments where scanning of the attachments did not complete. Because these two conditions will be defined in separate rules, the rules will be applied in a Boolean **OR** fashion (for example, condition 1 is True OR condition 2 is True).

This task will create the first rule; the next task will create the second rule.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. In your **Edge** browser, the **Exchange Admin Center** should still be open from the prior task, and you should still be on the **rules** tab for the **mail flow** page. If so, then proceed to the next step; otherwise, navigate to the **Exchange admin center**, then select **mail flow** in the left-hand navigation pane and select the **rules** tab, just as you did in the prior task.
3. In this task, you will create a mail flow rule that checks for emails that contain attachments that cannot be scanned. In the **rules** tab, select the **plus (+) sign** icon in the menu bar and in the drop-down menu, select **Modify messages.**
4. In the **new rule** window, enter **Attachments could not be scanned** in the **Name** field.
5. Select drop-down arrow in the **Apply this rule if...** field. In the menu that appears, review the available options. Note that in the default list of menu options, the only attachment-related option is **Any attachment's content includes**; there is no option related to the status of an attachment.

   Therefore, select inside the field to collapse the menu and then scroll down in the **new rule** window and select **More options...**
6. Scroll up to the top of the window. Select the drop-down arrow in the **Apply this rule if...** field. Hover your mouse over **Any attachment...** and in the menu that appears, select **content can't be inspected.**
7. Select the drop-down arrow in the **Do the following...** field. Hover your mouse over **Redirect the message to...** and in the menu that appears, select **hosted quarantine.**
8. Select the **add action** button to add another action.
9. Select the drop-down arrow in the second action field that appears. Hover your mouse over **Apply a disclaimer to the message...** and in the menu that appears, select **append a disclaimer.**
10. To the right of the second action field that displays **Append the disclaimer...,** select **Enter text.**
11. In the **specify disclaimer text** window, enter the following message in the field: **Attachments in this message were not scanned.**
12. Select **OK.**
13. To the right of the second action field that displays **Append the disclaimer...,** select **Select one.**
14. In the **specify fallback action** window, **Wrap** is displayed as the default fallback option. This is the option you want to select as the fallback option, so select **OK**.
15. Scroll down in the **new rule** window and under the **Properties of this rule** section, verify the **Audit this rule with severity level:** checkbox is selected. If it's not checked, then select it now.
16. Select the severity level drop-down arrow and select **Medium**.
17. In the **Choose a mode for this rule:** option, select **Enforce**.
18. Select **Save.**
19. This returns you to the **rules** tab in the Exchange admin center. The new **Attachments could not be scanned** rule should be displayed in the list of rules. This rule should be selected, and an **Attachments could not be scanned** pane should appear that displays the conditions and actions of this rule. Verify the conditions and actions are correct; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
20. Leave the Exchange Admin Center open to the mail flow page and proceed to the next task.

8.3 Task 3 - Create second Mail Flow rule for attachments

In the prior task, you created a mail flow rule for messages with attachments that were not scanned. In this task, you will create a second mail flow rule for messages with attachments; however, in this case, it will be for messages with attachments in which scanning of the attachments did not complete. Because these conditions will be defined in separate rules, the rules will be applied in a Boolean OR fashion.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. If the **Exchange admin center** is still open from the prior task, then proceed to the next step; otherwise, navigate to the **Exchange admin center**, then select **mail flow** in the left-hand navigation pane and select the **rules** tab.
3. You will now create a mail flow rule that checks for emails that contain attachments where the scanning of the attachments didn't finish. In the **rules** tab, select the **plus (+) sign** icon in the menu bar and in the drop-down menu that appears, select **Modify messages.**
4. In the **new rule** window, enter **Attachment scanning did not complete** in the **Name** field.
5. Scroll down and select **more options.** The reason you must select **More options** at this point in the process is that you want to apply this rule if an attachment was not scanned or the scanning didn't finish. However, as you saw in the prior task, those attachment options are not available in the initial **Apply this rule if...** condition field. You must select **More options** to see the attachment conditions.
6. Scroll up to the top of the window. Select the drop-down arrow in the **Apply this rule if...** field. Hover your mouse over **Any attachment...** and in the menu that appears, select **didn't complete scanning.**
7. Select the drop-down arrow in the **Do the following...** field. Hover your mouse over **Redirect the message to...** and in the menu that appears, select **hosted quarantine.**
8. Select the **add action** button to add another action.
9. Select the drop-down arrow in the second action field that appears. Hover your mouse over **Apply a disclaimer to the message...** and in the menu that appears, select **append a disclaimer.**
10. To the right of the second action field that displays **Append the disclaimer...,** select **Enter text.**
11. In the **specify disclaimer text** window, enter the following message in the field: **Scanning of attachments in this message did not complete.**
12. Select **OK.**
13. To the right of the second action field that displays **Append the disclaimer...,** select **Select one.**
14. In the **specify fallback action** window, **Wrap** is displayed as the default fallback option. This is the option you want to select as the fallback option, so select **OK**.
15. Scroll down in the **new rule** window and under the **Properties of this rule** section, verify the **Audit this rule with severity level:** checkbox is selected. If it's not checked, then select it now.
16. Select the severity level drop-down arrow and select **Medium**.
17. In the **Choose a mode for this rule:** option, select **Enforce**.
18. Select **Save.**
19. This returns you to the **rules** tab in the Exchange admin center. The new **Attachment scanning did not complete** rule should be displayed in the list of rules. This rule should be selected, and an **Attachment scanning did not complete** pane should appear that displays the conditions and actions of this rule. Verify the conditions and actions are correct; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
20. Leave the Exchange Admin Center open and proceed to the next task.

8.4 Task 4 – Create Mail Flow rule restricting email size

After Holly reviewed the messaging environment at Adatum Corporation, she realized that she could provide a more efficient and secure environment by creating some targeted mail flow rules. She has decided to create a set of mail flow rules that identify and act on messages that are in-transit through her Exchange Online

organization, as opposed to simply waiting until the messages are delivered to mailboxes before being acted upon by Inbox rules in Outlook and Outlook on the web.

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

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. If the **Exchange admin center** is still open from the prior task, then proceed to the next step; otherwise, navigate to the **Exchange admin center**, then select **mail flow** in the left-hand navigation pane and select the **rules** tab.
3. You will now create a mail flow rule that checks the size of emails and restricts those that exceed a specific size. In the **rules** tab, select the **plus (+) sign** icon in the menu bar and in the drop-down menu that appears, select **Filter messages by size.**
4. In the **new rule** window, enter **Email size restriction** in the **Name** field.
5. Select the drop-down arrow in the **Apply this rule if...** field. Hover your mouse over **The message...** and in the menu that appears, select **size is greater than or equal to.**
6. To the right of this condition field that displays **The message size is greater than or equal to...**, select **Enter text**.
7. In the **specify size (KB)** window, enter **1024** and then select **OK**.
8. Select the drop-down arrow in the **Do the following...** field. Hover your mouse over **Block the message...** and in the menu that appears, select **reject the message and include an explanation**.
9. In the **specify rejection reason** window that appears, enter the following text: **Your message exceeds the size limit. Please adjust the message size or compress the email content and send it as a zipped file.**
10. Select **OK.**
11. Scroll down to the **Choose a mode for this rule:** option and select **Enforce**.
12. Select **Save.**
13. This returns you to the **rules** tab in the Exchange admin center. The new **Email size restriction** rule should be displayed in the list of rules. This rule should be selected, and an **Email size restriction** pane should appear that displays the conditions and actions of this rule. Verify the conditions and actions are correct; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
14. Leave the Exchange Admin Center open to the mail flow page and proceed to the next lab.

9 End of Lab 2

10 Module 3 – Lab 3 - Exercise 1 - Create Hygiene Filters

In this lab, you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Adatum has experienced a recent rash of malware infections. The company's CTO has asked Holly to investigate the various options that are available in Exchange Online to fortify Adatum's messaging environment. Holly will begin by creating a series of hygiene filters that are designed to protect Adatum's messaging environment. You will create a malware filter, a connection filter, and a spam filter.

Note: In this lab exercise, you will use the **Office 365 Security and Compliance center** to create hygiene filters. Protection services no longer reside in the EAC for Exchange Online, and instead have been moved to the Security and Compliance center.

10.1 Task 1 - Create a Malware Filter

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

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. In your **Edge** browser, you should still have a tab open for the **Microsoft 365 admin center**. If so, then select this tab and proceed to the next step; otherwise, navigate to the **Office 365 home** page, log in as your tenant admin account, navigate to the **Microsoft 365 admin center**, and then in the left-hand navigation pane, select **Show all**.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane under **Admin centers**, select **Security**.
4. In the **Office 365 Security & Compliance center**, select **Threat Management** in the left-hand navigation pane, and then in the expanded group select **Policy**.
5. In the **Home > Policy** page, select the **Anti-Malware** tile under the **Policies** section.
6. In the **Home > Policy > Anti-malware** page, on the menu bar at the top of the window, select **+Create** to add a new malware filter. This initiates the **Create an anti-malware policy** wizard.
7. In the **Name your policy** page, enter **Malware Policy** in the **Name** field.
8. In the **Description** field, enter **This policy has been created to protect the messaging environment** and then select **Next**.
9. On the **Malware detection response** page, select **Yes and use the default notification text** then select **next**.
10. On the **Common attachment types filter** page, select **On - Emails with attachments of filtered files types will trigger the malware detection response (recommended).**
11. The filter will check for all the file types that appear in the **File Types** list. You do not need to add any additional file types, so proceed to the next step by selecting **Next**.
12. On the **Malware Zero-hour Auto Purge** page, confirm that the **On (recommended)** option is selected and then select **Next**.
13. On the **Notifications** page, since this filter will not generate any notifications, do not select any of the notification options, and instead select **Next**.
14. On the **Applied To** page, select the **Add a condition** button and in the drop-down menu that appears, select **The recipient domain is**.
15. If a pop-up window displaying domains appears, then skip to the next step; otherwise, to the right of the condition field that displays **The recipient domain is...,** select **A recipient's domain is.**
16. In the **The recipient's domain is** field, select **Choose**.
17. In the **The recipient domain is** page, select the **+Add** button. In the list of Adatum domains that appears, select the check box for the **xxxxxZZZZZZ.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), select the **Add** button, and then select **Done**.
18. On the **Applied To** page, the **xxxxxZZZZZZ.onmicrosoft.com** domain should appear in the **The recipient's domain is** field. Select **Next.**
19. On the **Review your settings** page, review the settings that you just configured. If anything needs to be corrected, select the corresponding **Edit** option to make the necessary fix. If everything is correct, select the **Create this policy** button at the bottom of the page.

    Note: A **Security & Compliance** window will appear with a message that indicates your organization settings need to be updated. Select **Yes** to continue.
20. It may take a minute or so for your organization settings to be updated. Once the update is complete and you are back on the **Home > Policy > Anti-malware** page, you can proceed to the next task. Do not close any of the browser tabs.

10.2 Task 2 - Create a Connection Filter

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

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. In your **Edge** browser, you should still be in the **Office 365 Security & Compliance center** (SCC). If so, then proceed to the next step; otherwise, perform the steps from the prior task to navigate to the SCC now.
3. In the **Office 365 Security & Compliance admin center**, select **Threat Management** in the left-hand navigation pane, and then in the expanded group select **Policy**.
4. In the **Home > Policy** page, select the **Anti-spam** tile under the **Policies** section.
5. In the **Anti-spam settings** window, in the list of policies, select the drop-down arrow to the left of **Connect filter policy (always ON)** and then select the **Edit policy** button that appears.
6. On the **Connection filter policy** pane, you can identify the IP Addresses that can send messages to your environment and the IP addresses will be blocked from sending messages.

   Note: At this time, you will NOT be adding IP addresses to the allow or block lists. You can do this if you have a known IP address you would like to test against. However, it typically takes up to 1 hour to propagate the change within the system. For this lab, simply review the fact that you can create allowed and blocked lists of IP addresses in this **Connection filter policy** pane.

   On the **Connection filter policy** pane, select the **Turn on safe list** check box at the bottom of the page.

   Important: Selecting the **Turn on safe list** check box is a best practice that enables for your Microsoft 365 tenant the most common third-party sources of trusted senders to which Microsoft subscribes. Selecting this check box skips spam filtering on messages sent from these senders, ensuring that they are never mistakenly marked as spam.
7. Select **Save**.
8. Leave the Office 365 Security & Compliance center open in your browser and proceed to the next task.

10.3 Task 3 - Create a Spam Filter

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

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

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. In your **Edge** browser, you should still be in the **Office 365 Security & Compliance center** (SCC). If so, then proceed to the next step; otherwise, perform the steps from the prior task to navigate to the SCC now.
3. In the **Office 365 Security & Compliance center**, you should still be on the **Anti-spam settings** page after completing the prior task. If so, then proceed to the next step; otherwise, in the left-hand navigation pane, select **Threat Management**, select **Policy,** and then select the **Anti-spam** tile under the **Policies** section.
4. In the **Anti-spam settings** window, in the list of policies, select the drop-down arrow to the left of **Default spam filter policy (always ON)** and then select the **Edit policy** button that appears.
5. In the **Default spam filter policy (always ON)** pane, you will be presented a variety of options on how you would like spam to be handled and what rating will be triggered depending on the severity of

the spam. The following steps will guide you through these settings so that you can update them per Adatum's requirements.

6. Select the **Spam and bulk actions** drop-down arrow and update the following settings:
   - Spam: **Move message to Junk Email folder**
   - High confidence spam: **Prepend subject line with text**
   - Phishing email: **Move message to Junk Email folder**
   - Bulk email: **No Action**
   - Select the threshold: **5**
   - Quarantine - Retain spam for (days): **10**
   - Prepend subject line with this text: enter **QUARANTINED: This message contains potential spam!**
7. Select the **International spam** drop-down arrow and update the following settings:

   Note: This section allows you to automatically tag as spam those messages sent from countries that are blocked, as well as messages written in a specific language.

   - Filter email messages written in the following languages:
     - Select **Edit.**
       - On the **International spam settings** pane, select the check box next to **Filter email messages written in the following languages.**
       - Type the letter **"a"** in the **Language** field to display the list of languages starting with the letter "a" or that include an "a".
       - Select any language you want to restrict.
       - If you want to restrict an additional language, repeat the prior two steps.
       - Once you have selected all the languages that you want to restrict, select **Save.**
       - Note how the value of the **Status** field has changed from **OFF** to **ON**.
   - Filter email messages sent from the following counties or regions:
     - Select **Edit.**
       - On the **International spam settings** pane, select the check box next to **Filter email messages sent from the following countries or regions.**
       - Type the letters **"ab"** in the **Language** field to display the list of languages starting with the letters "ab" or that include an "ab". You can enter any letter or letters that you wish.
       - Select any country/region you want to restrict.
       - If you want to restrict an additional country/region, repeat the prior two steps.
       - Once you have selected all the countries/regions that you want to restrict, select **Save.**
       - Note how the value of the **Status** field has changed from **OFF** to **ON**.
8. Select the **Spam properties** drop-down arrow and update the following settings:

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

   - Select the **Increase Spam Score** drop-down arrow and turn **On** the following options:
     - **URL redirect to other port**
     - **URL to .biz or .info websites**
   - Select the **Mark as Spam** drop-down arrow and turn **On** the following options:
     - **Empty messages**
     - **Conditional Sender ID filtering: hard fail**

9. Select **Save**.
10. In the list of spam filters, select the drop-down arrow to the left of the **Default spam filter policy (always ON)** filter that you just edited. In the middle column of settings for this filter, note how **End-user spam notifications** are disabled (it status is **Off**). Below this option, select **Configure end-user spam notifications**.
11. In the **Default** window that appears, select the **Enable end-user spam notifications** check box, and then change the **Send end-user spam notifications every (days)** value to **5**.
12. Select **Save**.
13. In your Edge browser, leave the **Office 365 Home** tab open as well as the **Microsoft 365 admin center** tab. Close all other tabs and proceed to the next lab.

11 End of Lab 3

12 Module 4 - Lab 4 - Exercise 1 – Managing Messaging Compliance

In this lab you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Holly has been tasked with maintaining message traffic and reducing the number of undeliverable emails in Adatum's messaging environment.

To complete this task, you will create data loss prevention policies and conduct message tracing to familiarize yourself with the tools provided by Microsoft 365 that assist you with managing message compliance.

12.1 Task 1: Prepare for eDiscovery

One of the significant security and compliance tools available in Microsoft 365 is the ability to perform eDiscovery searches on information gathered in the system. In the final task in this exercise, you will create an eDiscovery case that searches email messages for sensitive data. Once you create the case and perform a search associated with the case, you will attempt to view the search results.

eDiscovery cases can oftentimes hold sensitive information that may not be suitable for every administrator to review. To support this scenario, some Microsoft 365 administrator roles provide permission for users to create cases, but they do not include permission to view the search results. For example, a Compliance administrator can create an eDiscovery case and run an eDiscovery search, but unless the user is also assigned the new eDiscovery Manager role in the Security and Compliance center, he or she will be unable to view the search results. You will create this scenario in this lab excerise to verify this eDiscovery permission design.

In this task you will assign Nestor Wilke the Compliance administrator role. While this will enable Nestor to create an eDiscovery case for compliance purposes, it will not allow him to view the results of the corresponding search. To view the corresponding search results, Nestor would need to be assigned the eDiscovery Manager role.

Warning: The reason you will assign Nestor the Compliance administrator role now in Task 1 rather than later in Task 8 when you log in as Nestor is that it takes roughly 60 minutes for role assignments to fully propagate through the system. So hopefully by the time you get to Task 8, the role will be fully propagated, and you will be able to create an eDiscovery case.

1. You should still be logged into LON-CL1 as the **Administrator** with a password of **Pa55w.rd**; however, if the log-in page appears, then log in now.
2. In your **Edge** browser, you should still have a tab open for the **Microsoft 365 admin center**. If so, then select this tab and proceed to the next step; otherwise, repeat the steps that you performed in the earlier lab to navigate to the **Office 365 home** page and the **Microsoft 365 admin center.**
3. In the **Microsoft 365 admin center**, select **Users** in the left-hand navigation pane, and then in the expanded group select **Active users**.

   Note: 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 course, you are taking on the role of Holly Dickson, who uses the generic **MOD Administrator** account to sign into Microsoft 365 (using the tenant admin account of admin@xxxxxZZZZZZ.onmicrosoft.com). The MOD Administrator account has been assigned the Microsoft 365 Global admin role.

4. In the **Active users** window, select **Nestor Wilke's** account.

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

5. In the **Nestor Wilke** pane that appears, the **Account** tab is displayed by default. Scroll down and under the **Roles** section, select **Manage roles**.

6. On the **Manage roles** pane, note that Nestor is already assigned the Global admin role. The roles that appear under the **Admin center access** option are the most commonly assigned roles.

   Since the **Compliance admin** role that you want to assign to Nestor does not appear in this list of the most commonly assigned roles, scroll down and select **Show all by category**.

7. In the list of roles that are sorted by category, scroll down to the **Security & Compliance** category, select **Compliance admin**, and then select **Save changes**.

8. Select the **X** in the upper right corner of the **Manage roles** pane to close it.

9. Leave your browser open and proceed to the next task.

12.2 Task 2: Creating a Custom DLP policy

In this task your you will create a custom DLP Policy that prevents financial data from being sent out externally or internally. This policy will prevent users from sending emails that include credit card numbers, bank account numbers, and ABA routing numbers.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.

2. In your Edge browser, you should still have the **Microsoft 365 admin center** open from the prior task.

   In the left-hand navigation pane, select **Show All** (if necessary) to display all the navigation menu options, and then under the **Admin centers** section, select **Compliance.**

3. In the **Microsoft 365 compliance** portal, in the left-hand navigation pane, select **Policies.**

4. On the **Policies** page, under the **Data** section, select **Data loss prevention**.

5. On the **Data loss prevention** page, the **Policies** tab is displayed by default. On this tab, select **+Create policy** in the menu bar. This initiates the **Create policy** wizard.

6. In the **Start with a template or create a custom policy** page, the **Categories** column displays four major template groups, including Financial, Medical and health, Privacy, and Custom.

   Select **Financial**.

7. In the **Templates** column, scroll down and select **U.S. Financial Data** (be careful and do not select U.K. Financial Data).

8. Read the information provided in the **U.S. Financial Data** column that describes this template, and then select **Next.**

9. In the **Name your DLP policy** window, the template name of **U.S. Financial Data** is entered by default in the **Name** field, and a default description is entered in the **Description** field.

   While this DLP policy uses the U.S. Financial Data template, Holly wants to change the name to a more accurate value, since you will be modifying the rule that is created from this template to check for non-financial data as well (such as Driver's License Number and Passport Number).

   Change the value in the **Name** field to **U.S. PII Policy.**

   Note: PII stands for Personally Identifiable Information. It's a common IT industry acronym for the type of personal information tracked in this policy.

   Select **Next**.

10. On the **Choose locations to apply the policy** page, all the existing locations are turned **ON**. You only want the **Exchange email** location to be turned **ON**, so select the toggle switches for the remaining locations to turn them **OFF**, and then select **Next.**

11. On the **Define policy settings** page, the default option only includes the following default settings: Credit Card Number, U.S. Bank Account Number, and ABA Routing Number.

    However, Adatum also wants to include U.S. Driver's License Number, U.S. Social Security Number (SSN), U.S. / U.K. Passport Number, and U.S. Individual Taxpayer Identification Number (ITIN) in this DLP policy.

    To include these additional settings in this DLP policy, select the **Create or customize advanced DLP rules** option and then select **Next**.

12. In the **Customize advanced DLP rules** page, select **+Create rule**.
13. In the **Create rule** window, enter **Sensitive Data** in the **Name** field.
14. Under the **Conditions** group, select **+Add condition**.
15. In the menu that appears, select **Content contains.**
16. In the **Content contains** group and under the field that displays **Default**, select **Add**, and then in the drop-down menu that appears, select **Sensitive info types**.
17. In the **Sensitive info types** window, select the check boxes for the following types of information:
    - **ABA Routing Number**
    - **Credit Card Number**
    - **U.S. / U.K. Passport Number**
    - **U.S. Bank Account Number**
    - **U.S. Driver's License Number**
    - **U.S. Individual Taxpayer Identification Number (ITN)**
    - **U.S. Social Security Number (SSN)**
18. Select **Add**.
19. This returns you to the **Create rule** window. Scroll down and under the **Actions** group, select **+Add an action**. In the menu that appears, select **Restrict access or encrypt the content in Microsoft 365 locations**.
20. In the **Actions** group, select the check box next to the **Restrict access or encrypt the content in Microsoft 365 locations** option; this enables two options below it.
21. In the options that appear, verify the **Block users from accessing shared SharePoint, OneDrive, and Teams content** option is selected, and then under it, select the **Block everyone. Only the content owner, the last modifier and the site admin will continue to have access** option.
22. Scroll down on the **Create rule** window to the **User notifications** group. Select the toggle button to turn **ON** user notifications.
23. Under the **Email notifications** group, select the **Notify these people** option.
24. Under the **Notify these people** option, only **The person who sent, shared, or modified the content** check box is selected. Select the other two check boxes as well (**Owner of the SharePoint site or OneDrive account**, and **Owner of the SharePoint site or OneDrive content**).
25. Under the **Send the email to these additional people** group, select **Add or remove people**.
26. In the **Add or remove people** window that appears, select **MOD Administrator** from the list of users and then select **Add**.
27. This returns you to the **Create rule** window. Below the **Add or remove people** option that you previously selected are two check boxes, one to **Customize the email text** and the other to **Customize the email subject**.

    Select the **Customize the email text** check box.

28. Copy the following text and paste it into the field that appears below the **Customize the email text** check box:

WARNING: This email contains sensitive personal and/or corporate information that is not allowed to be included in emails. Please remove the sensitive information. Thank you.

29. In the **Create rule** window, scroll down to the **Incident reports** section. Select the drop-down arrow in the **Use this severity level in admin alerts and reports** field and select **High**.
30. Select the toggle button for the **Send an alert to admins when a rule match occurs** option to turn it **On**.
31. Scroll to the bottom of the **Create rule** window, select the drop-down arrow in the **Priority** field and select **1**.
32. Select **Save**.
33. This returns you to the **Customize advanced DLP rules** page. Select **Next**.
34. On the **Test or turn on the policy page**, select the **Yes, turn it on right away** option and then select **Next**.
35. On the **Review your policy and create it** page, review all your settings. If any setting needs correction, select **Back** as many times as needed to return to the page that requires correction, make your updates, and then select **Next** as needed to bring you back to this page.

    Once everything on this **Review your policy and create it** page is correct, select **Submit**.
36. On the **New policy created** window, select **Done**.
37. In the **Data loss prevention** window, the new policy that you just created should be displayed in the list of data loss prevention policies.

    IMPORTANT: Although the status of the policy is **Enabled**, it can take up to 24 hours for the policy to propagate through the system and become fully operational. Therefore, you cannot test the policy at this time to validate that it is working properly.

12.3 Task 3: Confirming the Status of the Custom DLP policy

In the prior task, you created a custom DLP policy. The task also indicated that it can take up to 24 hours for the policy to become active (i.e. to propagate through the system and become fully operational). In this task, you will learn how to use PowerShell to check the progress of the policy to determine when it is active.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. Select the magnifying glass on the taskbar at the bottom of the screen and enter **Powershell** in the Search box. In the menu that appears, right-click on **Windows PowerShell** (do NOT select Windows PowerShell ISE) and select **Run as administrator**.

   Maximize your Windows PowerShell window.
3. At the command prompt, run the following command to change the PowerShell execution policy for your Windows computer:

   Note: Instead of typing each command, it will be quicker to copy each command and paste it into PowerShell at the command prompt. Copy and pasting the commands will also avoid any errors that can occur when typing in the commands, especially with the longer commands. Your instructor will guide you on how to copy and paste text into your particular VM environment.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   Note: You will be prompted as to whether you want to change the execution policy. Enter **A** for **Yes to All.**
4. At the command prompt, run the following command to prompt you for your user credentials:

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

   Note: This will open a dialog box to enter your credentials. Enter **admin@xxxxxZZZZZZ.**

onmicrosoft.com (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **User name** field and enter your tenant email password in the **Password** field. Select **OK**.

5. At the command prompts, run the following two commands to establish your connection to the Security and Compliance center:

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.compliance
-Credential $UserCredential -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session -DisableNameChecking
```

6. At the command prompt, run the following command to display the Distribution Status of the DLP policy that you created in the prior task titled **U.S. PII Policy:**

```
Get-DlpCompliancePolicy "U.S. PII Policy"| select DistributionStatus
```

Note: At this moment, the **Distribution Status** of the DLP policy should be **Pending**, since it can take up to 24 hours before the policy becomes fully operational. In a real-world environment, you should check the status from time to time to verify when the Distribution Status changes to **Success**, which indicates the policy is active.

7. Minimize the Windows PowerShell window as you will use it in a later task.
8. Leave your Edge browser open and proceed to the next task.

12.4 Task 4: Performing a Message Trace

In this task, Holly Dickson plans to test Microsoft 365's message tracing functionality. Message traces are used to track and monitor where the message has traveled and what type of anti-spam and regulatory policies are enacted upon the message.

While you can start a trace at any time, it can be more efficient to run a trace based on an existing query so that you don't have to define the query parameters each time you run it. As part of her pilot project, Holly wants to begin by selecting a default query, which she will then customize.

Holly wants to send an email to Alex Wilber and then create a custom query that checks for emails sent in the past day to Alex from within the Adatum domain. After creating this custom query, you will run the query which will write the search results to a Message trace report and download the message trace results to a CSV file that will be sent in an email to the MOD Administrator.

Note: Message trace functionality was originally in the Office 365 Security and Compliance Center (SCC) and the classic Exchange (Online) admin center (EAC). It has since been moved to the New Exchange Online admin center, and it's in the process of being retired from the SCC and the classic EAC. For the purpose of this labs, you will use the message trace functionality in the New EAC.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In Edge browser, if you still have tabs open for the **Microsoft Office Home** page and the **Microsoft 365 admin center**, then proceed to the next step; otherwise, navigate to **https://portal.office.com**, log in as **admin@xxxxxZZZZZZ.onmicrosoft.com** with the tenant email password, and then select **Admin**.
3. Select the **Microsoft Office Home** tab and then select **Outlook** to open **Outlook on the web** for the MOD Administrator's account.
4. You will begin by sending an email to Alex Wilber. In the upper left corner of the screen, select **New message**.
5. In the message pane that appears on the right-side of the screen, enter the following information:
   - To: start typing **Alex** and a drop-down menu displays with users whose name begins with Alex. Select **Alex Wilber**.
   - Add a subject: **Confidential message tracing test**

- Message area: **This message will be used to test the message trace tool located in the new Exchange admin center when you search for the words confidential, sensitive, and secret in emails.**

  Important: In a later task, you will search for emails that include the words Confidential, Sensitive, and Secret. Therefore, enter (or copy and paste) in the message included above so that that you can test whether it is captured in the search.

6. Select **Send**.
7. You will now create a custom message trace query and report in the New Exchange admin center. In your **Edge** browser, select the **Microsoft 365 admin center** tab.
8. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Show all** (if necessary) and under **Admin centers,** select **Exchange**.
9. The Message Trace functionality has been moved to the **New Exchange admin center**. Therefore, in the (classic) **Exchange admin center**, in the left-hand navigation pane, select **New Exchange admin center.**
10. In the (New) **Exchange admin center**, in the left-hand navigation pane, select **Mail flow** and then select **Message trace**.
11. On the **Message trace** page, the **Default queries** tab at the top of the page is displayed by default. In the list of queries and reports in this tab, select **Messages sent from my primary domain in the last day.**
12. In the **New message trace** pane that appears, the default values for the **Messages sent from my primary domain in the last day** query are displayed. You can control which messages are selected based on who sent and received the messages and how many days ago the messages were sent.

    Starting with this default query as a template, Holly will now customize its settings to create a custom query that checks for emails sent to Alex Wilber in the past day.

    - You can customize the **Senders** field to search for messages that were sent from a specific domain. By default, the query will select messages sent from all Adatum user accounts in its Microsoft 365 tenant; that is, from all user accounts whose primary domain matches Adatum's tenant of **@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the unique tenant prefix provided by your lab hosting provider). Therefore, do NOT change this value.

      - You can customize the **Recipients** field to search for messages that were sent to specific users. By default, the query will select messages sent to all recipients. However, Holly wants to modify the query to only select messages sent to Alex Wilber. Therefore, enter **Alex** in the **Recipients** field, and then in the menu of users that appears, select **Alex Wilber.**
13. To avoid issues with the starting time for the search, on the **Time range** slider tool, drag the slider to the left so that it specifies sometime in the **Last 2 days** (actually, you can select any value greater than 1 day).
14. Under the **Report type** section, select the **Extended report** option and then select **Next**.
15. On the **Prepare message trace report** page, review the information for the report you just configured.

    Select the **Prepare report** button at the bottom of the pane.
16. On the **Your request has been submitted** page, review the information and then select **Close**.
17. On the **New message trace** window, select **Save**.
18. In the dialog box that appears, change the **Name** of the report to **Messages sent to Alex Wilber in the past day**, select **Save**, and then select **Done**.
19. In the **New message trace** pane, select the **X** in the upper right-hand corner to close the pane.
20. On the **Message trace** window, note how the **Custom queries** tab is now displayed, and it includes the **Messages sent to Alex Wilber in the past day** query that you just created. Holly has now created a custom query that she can run at any time in the future.

    Since Holly wants to test this custom query, select the **Messages sent to Alex Wilber in the past day** query (select the **Name** and not the circle with the check mark to the left of the name).

21. In the **New message trace** window, note how the query values are prefilled for you. Select **Next**.
22. On the **Prepare message trace report** pane, select the **Prepare report** button at the bottom of the window.
23. On the **Your request has been submitted** pane, review the information on the page, including the following messages:

    You can check progress at any time from the "Downloadable reports" section on the Message Trace home page.
    and
    When the report is ready to download the email below will be notified: admin@xxxxxZZZZZZ.onmicrosoft.com

    Select **Close.**
24. Close the **New message trace** window.
25. On the **Message trace** page, the **Downloadable reports** tab will be displayed. This will display the **Message trace report** that you just ran. Note that its **Status** will initially be **Not started**.

    Select the **Refresh** icon on the address bar every minute or so to check on the report's status (the status should transition from **Not started** to **In progress** to **Complete**).

    Note: Refreshing the page will cause it to display the **Default queries** tab; therefore, each time you refresh the page, you must select the **Downloadable reports** tab to check the report status.

    WARNING: In the testing of this lab, the message trace report sometimes took up to an hour or more to complete. If the report does not finish after a few minutes, review the remaining steps in this task so that you can see what you would have done, and then perform the final step in this task before proceeding to the next task.
26. You will receive a notification once the report is complete. You should notice this in the **notification bell** that appears at the top right of the screen (it will display a number that indicates the number of notifications you have).

    When you see a 1 in the notification bell, select the bell to display the **Notifications** pane. In the **Notifications** pane, select the email entry.
27. The query that you created was designed to send an email to the MOD Administrator that included a link to the Message trace report. In the email window that appears, in the middle of the email you should see a statement that says **You can access the report here** (where "**here**" is hyperlinked). Select this hyperlinked "**here**" to view the results.
28. As the system attempts to open the report, it will display a notification bar that asks whether you want to open or save the .csv file associated with the report. Select **Save.**

    This file contains all corresponding information from the email, including but not limited to: SCL, Number of hops, source IP address, what connector used, delivery priority. Most of the information will be located in the custom data column.

    Congratulation! You have just verified the message trace report was created, the MOD Administrator was notified in an email that the report was complete, and the CSV file with the report results was made available for downloaded by the MOD Administrator.
29. In your Edge browser, leave the **Office 365 Home** tab open, as well as the **Microsoft 365 admin center** tab. Close all other tabs and proceed to the next task.

12.5 Task 5: Reviewing Active MRM Policies with PowerShell

In this task you will run a series of Windows PowerShell commands to review the active MRM policies in Adatum's Exchange environment.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. The **Windows PowerShell** console should still be open from the earlier task in which you verified the status of your custom DLP policy; if so, then select the **PowerShell** icon on the taskbar to maximize the window.

If you closed the PowerShell window in the earlier task, then repeat the steps you performed previously to open an elevated instance of PowerShell.

3. In **Windows PowerShell**, run the following command at the command prompt to install the new Exchange Online module:

   Note: Instead of typing each command, it will be quicker to copy each command and paste it into PowerShell at the command prompt. Copy and pasting the commands will also avoid any errors that can occur when typing in the commands, especially with the longer commands. Your instructor will guide you on how to copy and paste text into your particular VM environment.

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

4. You will be prompted whether you want PowerShell to install and import the NuGet provider. Enter **Y** for **Yes**.

5. You will then be prompted whether you want PowerShell to install the modules from PSGallery, which is an Untrusted Repository. Enter **A** for **Yes to All**.

6. At the command prompt, run the following command to connect you to the Exchange admin center for Exchange Online:

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

   Note: If you closed PowerShell after running it in the earlier task, you will receive a **Sign in** dialog box to enter your credentials. Enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the unique tenant prefix provided by your lab hosting provider) and your tenant admin password. If your PowerShell session was still open, then you should not receive this **Sign in** window.

7. At the command prompt, run the following command to validate that you are connected to Exchange Online by displaying 5 mailboxes:

   ```
   Get-EXOMailbox -ResultSize 5
   ```

   Note: Review the **User Principal name** assigned to each mailbox to confirm you are connected to the right tenant.

8. At the command prompt, run the following command to display all the Retention Policies that are active in your environment:

   ```
   Get-RetentionPolicy | out-Gridview
   ```

   Note: This command opens a separate window that displays the active retention policies. After reviewing the policies, select the **X** in the upper right corner of the window to close it and return to the PowerShell command prompt.

9. At the command prompt, run the following command to display all the retention policy tags that are associated to the Default MRM Policy:

   ```
   (Get-RetentionPolicy "Default MRM Policy").RetentionPolicyTagLinks | Format-Table name
   ```

10. Close the Windows PowerShell window.

12.6 Task 6: Creating a Retention Label

In your role as Holly Dickson, Adatum's Messaging Administrator, you will continue with your task of reviewing Microsoft 365's compliance tools by creating a Retention label through the Security and Compliance portal.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.

2. In your **Edge browser**, select the **Microsoft 365 admin center** tab, and then in the left-hand navigation pane under **Admin centers**, select **Compliance.**

3. In the **Microsoft 365 compliance** center, in the left-hand navigation pane, select **Catalog**.

4. On the **Solution catalog** page, in the **Information protection & governance** section, select the **View** button under **Information governance**.
5. In the **Information governance** window, select **Open solution**.
6. In the **Information governance** window, the **Labels** tab at the top of the page is displayed by default. In this tab, select **+Create a label** that appears on the menu bar. This initiates the **Create a label** wizard.
7. On the **Name your label** page, enter **30-day delete** in the **Name** field, and enter **This label will delete email after 30 days** in the **Description for admins** field. Copy this description and paste it into the **Description for users** field. Select **Next**.
8. On the **Label settings** page, select the **Retention** toggle switch to turn it **On**. This turns on retention settings for this label, and it displays several additional settings. Configure these settings as follows:
   - Retain the content: **For this long – 30 Days**
   - What do you want to do after this time? **Delete the content automatically**
   - Retain or delete the content based on: **when it was created**
9. Select **Next**.
10. On the **Review your settings** page, review your settings and if any require correction, select the corresponding **Edit** option to fix the setting. When all settings are correct, select **Create this Label**.
11. It will take a minute or two to create the retention label, at which point the **Information governance** window will display your new **30-day delete** label.
12. Leave your browser and all tabs open and proceed to the next task.

12.7 Task 7: Creating a Retention Label Policy

In the prior task, you created a Retention Label. In this task, you will create a Retention Label Policy and assign it to the Retention Label that you previously created.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your **Edge browser**, you should still have the **Information governance** page open from the previous task. This page should be displaying the **Labels** tab, and in the list of labels, it should display the **30-day delete** label that you just created.

   Once you create a label, your next step is to publish it. You can either publish multiple labels at one time by selecting the **Publish labels** option on the menu bar, or you can publish a specific label by selecting the label and then publishing just that label.

   In this task, you will publish a specific label; therefore, in the list of labels, select the **30-day delete** label.
3. In the **30-day delete** window that appears, select the **Publish labels** button at the top of window. This will initiate the **Publish labels** wizard that walks you through the steps of publishing a label.
4. On the **Choose labels to publish** page, the **30-day delete** label is already displayed under the **Publish these labels** section since you previously selected this label; therefore, select **Next**.
5. On the **Choose locations** page, select the **All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents** option and then select **Next**.
6. On the **Name your policy** page, enter **30-day delete policy** in the **Name** field. Leave the **Description** field blank and select **Next**.
7. On the **Review you settings** page, review your settings and if any require correction, select the corresponding **Edit** option to fix the setting. When all settings are correct, select **Publish labels**.

   Important: Note the warning message that indicates it can take up to 1 day to propagate a new retention label policy throughout the system once the policy is published.
8. Once the retention label policy has been created, it will be displayed in the list of label policies on the **Retention labels** window.

9. Leave your browser and all tabs open and proceed to the next task.

12.8 Task 8: Creating an eDiscovery Case

In your role as Holly Dickson, Adatum's Messaging Administrator, you want to continue in your pilot project that examines Microsoft 365's compliance functionality. In this task, you will create an eDiscovery case that searches for confidential information being disseminated through email.

Because eDiscovery cases can oftentimes hold sensitive information that may not be suitable for every administrator to review, many organizations want to control who has permission to view eDiscovery search results. To support this scenario, some Microsoft 365 administrator roles provide permission for users to create eDiscovery cases, but they do not include permission to view the search results. Only the new eDiscovery Manager role that is assigned in the Security and Compliance center provides permission to view search results.

Back in Task 1, you assigned the Compliance administrator role to Nestor Wilke. While a Compliance admin can create an eDiscovery case and perform a corresponding search, the admin is not able to view the search results unless he or she is also assigned the eDiscovery Manager role. Because you assigned Nestor the Compliance admin role, he now has permission to create an eDiscovery case and initiate an eDiscovery search; however, since you did not assign him the eDiscovery Manager role, he does not have permission to view the search results. In this task, you will verify this permission design by logging in as Nestor, creating an eDiscovery case, initiating the search, and then validating what happens with the search results.

Note: It normally takes about 60 minutes for a new role assignment to fully propagate through the system. This is why you assigned Nestor the Compliance admin role in Task 1. By the time you reach this task, enough time should have passed for Nestor's new permissions to have propagated through the system, enabling him to create an eDiscovery case. If the role assignment you performed in Task 1 has not fully propagated, Nestor will be unable to create the eDiscovery case. If this occurs, determine how much longer you must wait until you reach an hour since you completed Task 1 and then perform this task again.

1. You should still be logged into LON-CL1 from the prior task; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. You must begin this task by signing out of Microsoft 365 as the MOD Administrator and then signing back in as Nestor Wilke.

   In your **Edge browser**, select the **Microsoft Office Home** tab, then select the MOD Administrator user icon in the upper right corner of the screen (the circle with **MA** in it) and select **Sign out** in the menu that appears.
3. Close all the tabs in your browser session except for the tab in which you signed out.
4. In your Edge browser, enter the following URL in the address bar to go directly to the Office 365 Security & Compliance center (Note: While you could have logged into the Office 365 Home page and then navigated to the Microsoft 365 admin center and then to the Security and Compliance center just as you did in the prior lab, this approach will give you experience navigating directly to the Security and Compliance center): **https://protection.office.com**
5. In the **Pick an account** window, select **Use another account**.
6. In the **Sign in** window, enter **NestorW@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and then select **Next.**
7. In the **Enter password** window, enter the tenant email password provided by your lab hosting provider and then select **Sign in**.
8. On the **Office 365 Security & Compliance** center, select **eDiscovery** in the left-hand navigation pane, and then in the expanded group select **eDiscovery.**
9. In the **eDiscovery** pane, select the **+Create a case** button.
10. In the **New case** pane that appears, enter **AlexWilber-case01** in the **Case name** field.

    In the **Case description** field enter (copy and paste) the following description: **This case searches for emails to Alex Wilber that include confidential information**.
11. Select **Save.**
12. On the **eDiscovery** window, in the list of cases, select the **Open** button that appears next to **AlexWilber-case01.**

13. A new tab will open in your browser that displays this case. On the menu bar at the top of the page, select the **Holds** tab.
14. In the **Holds** tab for this case, select the **+Create** button. This will initiate a **Create a new hold** wizard that walks you through the steps to create a new hold.

    You will begin by placing a hold on Alex Wilber's account that will retain any emails that contain **Sensitive, Confidential, Secret** anywhere in the email as well as in the Subject line.
15. In the **Create a new hold** window, in the **Name your hold** page, enter **AlexW** in the **Name** field, leave the **Description** blank, and then select **Next**.
16. In the **Choose locations** page, to the right of the **Exchange email** location, select **Choose users, groups, or teams.**
17. In the **Edit locations** page, under **Exchange email**, select the **Choose users, groups, or teams** button.
18. In the **Edit locations** page, enter **Alex** in the **Search** field that appears and select the **Search** (magnifying glass) icon to the right of the field. This will initiate a search of all users whose name starts with Alex. Scroll to the bottom of the **Edit locations** pane to view the search results.
19. Select the check box next to **Alex Wilber** and then select the **Choose** button at the bottom of the window.
20. On the **Edit locations** page, select **Done**.
21. On the **Choose locations** page, select **Next**.
22. On the **Query conditions** page, in the **Enter keywords** field, enter the following: **Sensitive, Confidential, Secret**
23. Select **+Add conditions**.
24. On the **Add conditions** pane that appears, scroll to the bottom of the pane and select the **Subject** check box (not the Subject/Title) and then select **Add.**
25. On the **Query conditions** page, in the **Subject** section, select the drop-down arrow in the first operator field and select **Contains any of**. In the **Type subject** field, enter the following: **Sensitive, Confidential, Secret**
26. Select **Next**.
27. On the **Review your settings** page, review the settings and if any need to be adjusted, select **Edit** next to the setting and make the necessary correction. Once all settings are correct, select **Create this hold**.
28. In the **AlexW** pane, select **Close**.

    Note: You have just placed a hold on Alex Wilber's account that will retain any emails that contain **Sensitive, Confidential, Secret** anywhere in the email as well as in the Subject line.
29. In the **AlexWilber-case01 > Core ED > Hold** page, select the **Searches** tab at the top of the page.

    You will now create a new search that checks for emails that contain **Sensitive, Confidential, Secret** in the email and in the Subject line.
30. In the **Searches** tab, select the **+Guided Search** button. This will initiate a **New search** wizard that walks you through the steps to create a new search.
31. In the **New search** window, in the **Name your search** page, enter **Confidential search** in the **Name** field, leave the **Description** field blank, and then select **Next**.
32. In the **Locations** page, select the **Specific locations** option and then select the **Select all** toggle switch that appears to the right of **Exchange email** to turn it **On.** Select **Next**.
33. In the **Condition card** page, in the **Enter keywords** field, enter the following: **Sensitive, Confidential, Secret**
34. Select **+Add conditions.**
35. On the **Add conditions** pane that appears, scroll to the bottom of the pane and select the **Subject** check box (not the Subject/Title) and then select **Add.**

36. On the **Condition card** page, in the **Subject** section, select the drop-down arrow in the first operator field and select **Contains any of**. In the **Type subject** field, enter the following: **Sensitive, Confidential, Secret**
37. Select **Finish**. This initiates the search. It may take several minutes for the Search to complete.
38. Review the search results. Because Nestor was not assigned the eDiscovery Manager role, he is unable to view the search results. Therefore, the following message should appear at the top of the screen: **To preview search results, please ask your Compliance admin to grant you Preview permission.**
39. Leave the Edge browser open and proceed to the next lab.

13 End of Lab 4

14 Module 6 – Lab 5 - Exercise 1 - Implement ActiveSync

In this lab you will be guided through the process of enabling and disabling Exchange ActiveSync. ActiveSync is a client protocol that enables users to synchronize their on-premises Exchange mailbox with a mobile device. In this lab, you will log into the Exchange Server VM (LON-EX1) and set up ActiveSync for a single on-premises mailbox as well as for multiple mailboxes using the Exchange Admin Center for Exchange Server 2019.

14.1 Task 1 - Create Recipient mailboxes

To enable and disable ActiveSync, you must first create several recipient mailboxes in the on-premises Exchange admin center (EAC) on the Exchange Server (LON-EX1) VM to facilitate this lab exercise. Holly Dickson, Adatum's new Messaging administrator, has decided to create on-premises mailboxes for herself and two new team employees, Paul Wimmer and Jessica Hofer.

1. Switch to **LON-EX1** where you should already be logged in as the **Administrator** with a password of **Pa55w.rd** from the Lab 1 exercise.
2. To create on-premises user mailboxes, you must open the on-premises Exchange admin center for Exchange Server 2019. To do so, select the **Start** icon on the taskbar, and in the Start menu select the **Microsoft Exchange Server 2019** group. In the program group, select **Exchange Administrative Center**.
3. This will open the **Edge** browser, which will display the sign-in page for the **Exchange admin center**. Sign into the EAC as **adatum\Administrator** and password **Pa55w.rd.**
4. In the **Exchange admin center**, in the left-hand navigation pane, select **recipients** if necessary (it should be selected by default).
5. On the **recipients** page, the **mailboxes** tab at the top of the page should be displayed by default.

   On the **mailboxes** tab, select the **plus (+) sign** icon and in the drop-down menu that appears, select **User mailbox.**
6. In the **new user mailbox** window, enter **hollyd** in the **Alias** field.
7. Select the **New User** option.
8. Enter **Holly** in the **First name** field.
9. Leave the **Initials** field blank.
10. Enter **Dickson** in the **Last name** field.
11. When you tab off the **Last name** field, **Holly Dickson** will be automatically displayed in the **Display name** and **Name** fields.
12. For the **Organizational unit** field, select the **Browse** button.
13. In the **select an organizational unit** window, select **Users** and then select **OK**.
14. Scroll down in the window and enter **hollyd** in the **User logon name** field.

    Note: The domain field (to the right of the **User logon name**) is prefilled with **Adatum.com**; this is Adatum's on-premises domain. Leave this set to **Adatum.com**.
15. Enter **Pa55w.rd** in the **New password** and **Confirm password** fields.

16. Make sure the **Require password change on next logon** check box is unchecked; if necessary, uncheck it.
17. Select **Save.** The new user mailbox that was created for Holly Dickson should be displayed in the list of mailboxes.
18. Repeat steps 5-17 for the following two users:
    - **Paul Wimmer**; alias and user log on name: **paulw**
    - **Jessica Hofer**; alias and user log on name: **jessicah**
19. Leave the Exchange admin center open and proceed to the next task.

14.2 Task 2 - Maintain ActiveSync For a Single Mailbox

By default, Exchange ActiveSync is enabled for all user mailboxes; therefore, all users who have an Exchange mailbox can synchronize their mobile device with the Microsoft Exchange server.

In this task, you will disable Exchange ActiveSync for Holly Dickson's mailbox. You will then repeat the process to enable ActiveSync for Holly. This provides you with experience in both disabling and enabling ActiveSync for a single mailbox.

1. You should still be logged into LON-EX1 as the **Administrator**, and you should have the EAC open in Edge browser; if not, then do so now.
2. In the **Exchange admin center**, you should still be displaying the **recipients** tab from the left-hand navigation pane, and you should be displaying the **mailboxes** tab at the top of the page; if not, then do so now.
3. In the list of recipient mailboxes, select **Holly Dickson**.
4. Select the **pen (Edit)** icon on the menu bar to edit the mailbox properties for Holly Dickson.
5. The **Edit User Mailbox** window will open for Holly Dickson. In the left-hand navigation pane, select **mailbox features**.
6. In the **Phone and Voice Features** section, under **Mobile Devices**, select **Disable Exchange ActiveSync**.
   Note: Because **Disable Exchange ActiveSync** appears, that indicates that ActiveSync is enabled for Holly's mailbox (which is the default for new mailboxes).
7. A **Warning** dialog box appears asking whether you're sure you want to disable Exchange ActiveSync for this mailbox. Select **Yes**.
8. Repeat steps 4-8 for Holly's mailbox, but this time under the **Mobile Devices** section, note that **Disable Exchange ActiveSync** has now been changed to **Enable Exchange ActiveSync**. This indicates that ActiveSync is now disabled for Holly's mailbox. When repeating these steps, this time select **Enable Exchange ActiveSync.**

   Note: Under the **Mobile Devices** section, **Enable Exchange ActiveSync** is changed back to **Disable Exchange ActiveSync**, which indicates that ActiveSync is once again enabled for Holly. Also note how ActiveSync was enabled without displaying a Warning message asking you to verify that you wanted to enable it. That's the only difference between enabling and disabling ActiveSync.
9. Leave the Exchange Admin Center open for use in the next task.

14.3 Task 3 - Maintain ActiveSync For a Multiple Mailboxes

In this task, you will begin by disabling Exchange ActiveSync for a group of mailboxes. You will then repeat the process, but this time you will enable ActiveSync for this same set of mailboxes. This provides you with experience in both disabling and enabling ActiveSync for multiple mailboxes at one time.

1. You should still be logged into LON-EX1 as the **Administrator**, and you should have the EAC open in Edge browser; if not, then do so now.
2. In the **Exchange admin center**, you should still be displaying the **recipients** tab from the left-hand navigation pane, and you should be displaying the **mailboxes** tab at the top of the page; if not, then do so now.

3. In the list of recipient mailboxes, select **Paul Wimmer**. Note how the details pane on the right-hand side of the page displays the details for Paul's mailbox.
4. Hold down the CTRL key and select **Jessica Hofer**. Note how the title of the details pane on the right-hand side of the page changes to **Bulk Edit**.
5. In the **Bulk Edit** detail pane, scroll down to **Exchange ActiveSync** and select **Disable.**
6. A **bulk disable Exchange ActiveSync** pop-up window appears asking whether you're sure you want to disable Exchange ActiveSync for these selected recipients. Select **OK**.
7. Repeat steps 5-6, but this time under **Exchange ActiveSync,** select **Enable.**
8. Leave the Exchange Admin Center open for use in a future lab exercise.

15 End of Lab 5

16 Module 7 - Lab 6 - Exercise 1 - Manage Roles and Permission Policies

In this exercise you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Holly has been tasked with managing Microsoft 365 admin roles and permission policies for Adatum's Microsoft 365 messaging environment. The CTO has asked Holly to create a new Microsoft 365 management role group that allows an administrator to remotely access a mailbox without having the password.

In this exercise Holly will access the Exchange admin center for Exchange Online from her client computer (LON-CL1).

16.1 Task 1 - Create an Admin Role

A management role group is a universal security group used in the Role Based Access Control (RBAC) permissions model for Exchange Online. A management role group simplifies the assignment of management roles to a group of users. All members of a role group are assigned the same set of roles. After the role group is added, the members of the role group are granted the permissions provided by the roles assigned to the role group.

In this task, you are going to create a custom role group and then assign multiple roles to it. In this task, you will create an admin role that allows an administrator to remotely access a mailbox without having the password. You will then assign two specific administrators to this role.

1. Switch to the LON-CL1 VM and if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. The Microsoft Edge browser should still be open from Lab 4 where you were logged into Microsoft 365 as Allan Deyoung and you had the Office 365 Security & Compliance center open. You must log out of Microsoft 365 as Allan and log back in as the MOD Administrator account so that Holly can manage the Exchange admin roles and permissions.

   On the **Office 365 Security & Compliance** center tab, select Allan's picture in the upper right-hand corner of the screen, and in the menu that appears, select **Sign out**.
3. Close all tabs in the Edge browser except for the **Sign out** tab.
4. On the **Sign out** tab, enter the following URL in the address bar: **https://portal.office.com**
5. On the **Pick an account** window, select **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider). On the **Enter password** window, enter the tenant admin password provided by your lab hosting provider and then select **Sign in**.
6. On the **Office 365 home** page, select the **Admin** icon in the column of Microsoft 365 app icons on the left-side of the screen.
7. On the **Microsoft 365 admin center**, select **Show all** in the left-hand navigation pane, and then under **Admin centers**, select **Exchange.**
8. In the **Exchange admin center** tab, in the left-hand navigation pane, select **permissions.**
9. At the top of the **permissions** page, the **admin roles** tab should be displayed by default; if not, then select it now.

10. The **admin roles** window displays the existing role groups. Each of these groups has one or more roles assigned to it.

    For example, the **Compliance Management** role group is highlighted by default as it's the first group in the list. In the details pane on the right-hand side of the screen, it displays the properties for this role group, which includes the roles and members that have been assigned to it. In this task, you are going to create a custom role group and then assign multiple roles to it, as well as several existing members.

    Select the **plus (+) sign** icon on the menu bar to create a new role group.

11. In the **new role group** window, enter **Application Impersonation** in the **Name** field.

12. Enter (copy and paste) the following text into the **Description** field: **This role group allows an administrator to remotely access a mailbox without having the mailbox owner's password.**

13. Under **Roles**, select the **plus (+) sign** icon to assign roles to the group.

14. In the **Select a Role** window, you want to add the following roles to this role group. The easiest way to do this is to select the first role (ApplicationImpersonation), then hold down the CTRL key and select the remaining two roles:

    - **ApplicationImpersonation**
    - **Mail Recipients**
    - **UserApplication**

15. Select the **add ->** button, verify that all three roles appear in the field, and then select **OK**.

16. In the **new role group** window, scroll down the to the **Members** section and select the **plus (+) sign** icon to assign members to the group.

17. In the **Select Members** window, you want to add the following users to this role group. The easiest way to do this is to select the first user (Admin), then hold down the CTRL key and select the remaining user:

    - **Admin**
    - **TenantAdmins_-##########** (where ########## represents the tenant number at the end of the TenantAdmins group)

18. Select the **add ->** button, verify that both users appear in the field, and then select **OK**.

19. Select **Save**.

20. This returns you to the **admin roles** tab in the Exchange admin center. The new **Application Impersonation** role group should be displayed in the list of groups. This role group should be selected, and an **Application Impersonation** pane should appear on the right-side of the page that displays the details of this group.

    Verify the information is correct; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.

    Important: Even though the **Application Impersonation** group appears in the list of role groups, it typically takes 24 to 48 hours to fully propagate changes to the permission configuration.

21. Leave the Exchange Admin Center open and proceed to the next task.

16.2 Task 2 - Manage an Admin Role

In the prior task, you created a custom role group and added roles to the role group. In this task, you are going to add a user to a role group.

1. You should still be logged into LON-CL1 as the **Administrator** account with a password of **Pa55w.rd**; however, if the log-in screen appears, then log in now.

2. The **Exchange admin center** for Exchange Online should still be open in your Edge browser. You should still be on the **permissions** page, which should be displaying the **admin roles** tab from the prior task.

    In the list of admin role groups, select the **Discovery Management** role group.

3. Select the **pencil (Edit)** icon to on the menu bar to edit this group.

4. In the **Discovery Management** window, scroll down to the **Members** section and then select the **plus (+) sign** icon to add new members to this role group.
5. In the **Select Members** window, select **admin** (this is the MOD Administrator user account).
6. Select the **add ->** button and then select **OK**.
7. Select **Save**.
8. This returns you to the **admin roles** tab on the **permissions** page. The **Discovery Management** role group should be displayed in the list of groups. This role group should be selected, and a **Discovery Management** pane should appear that displays the details of this group.

   Verify the **MOD Administrator** user account appears under the list of **Members**; if any corrections are needed, select the **pencil (Edit)** icon in the menu bar and make the necessary corrections.
9. Leave the Exchange Admin Center open in your Edge browser and proceed to the next task.

16.3 Task 3 -Create an Outlook Web App Policy

A mobile device mailbox policy allows you to apply a common set of security and mobile device settings to a group of users. You can create multiple mobile device mailbox policies. Each recipient in your organization must have a mobile device mailbox policy assigned to them. When you install Microsoft Exchange Server 2013 or later, a default mobile device mailbox policy is created, and new users are automatically assigned this policy.

In this task, you will create a new Outlook Web App policy that will later be assigned to several test users in Holly's pilot project.

1. You should still be logged into LON-CL1 as the **Administrator** account with a password of **Pa55w.rd**; however, if the log-in screen appears, then log in now.
2. The **Exchange admin center** for Exchange Online should still be open in your Edge browser. You should still be on the **permissions** page from the prior task. At the top of the **permissions** page, select the **Outlook Web App policies** tab.
3. In the list of Outlook Web App policies, the **OwaMailboxPolicy-Default** policy is the only current policy. By default, this policy is assigned to all user mailboxes.
4. To create a new Outlook Web App policy, select the **plus (+) sign** icon on the menu bar.
5. In the **new Outlook Web App mailbox policy** window, enter **Test OWA Mailbox policy** in the **Policy name** field.
6. In the **Communication Management** group, all features are selected by default. Select the **Unified Messaging** check box to unselect it.
7. In the **Information management** group, un-check **Journaling**.
8. In the **User experience** group, select **Places** and **Local events**.
9. Select **Save** and then select **OK** once the information is successfully saved. Your new custom policy should appear in the list of Outlook Web App policies.
10. Leave the Edge browser and all tabs open and proceed to the next exercise.

16.4 Task 4: Assign an Outlook Web App Policy to a user mailbox

Assigning an Outlook on the web mailbox policy to an Exchange Online mailbox controls the Outlook on the web (formerly known as Outlook Web App, or OWA) experience for the user. You can apply Outlook on the web mailbox policies to one or more mailboxes or remove the policy assignments in the Exchange admin center (EAC) or Exchange Online PowerShell.

In this task, you are going to assign the Outlook Web App policy that you created in the prior task to the mailboxes of three Adatum users who are part of Holly's pilot project.

1. You should still be logged into LON-CL1 as the **Administrator** account with a password of **Pa55w.rd**; however, if the log-in screen appears, then log in now.
2. The **Exchange admin center** for Exchange Online should still be open in your Edge browser. In the left-hand navigation pane, select **recipients.**

3. On the **recipients** page, the **mailboxes** tab should be selected by default; if not, then select it now.
4. The prior task indicated that by default, all user mailboxes are assigned the **OwaMailboxPolicy-Default** policy. Let's verify this before assigning the new policy to one of the user mailboxes. In the list of Microsoft 365 user account mailboxes that were created by your lab hosting provider, select **Joni Sherman**.
5. In the **Joni Sherman** detail pane on the right, scroll to the bottom of the pane and in the **Email Connectivity** section, select **View details**.
6. An **Outlook Web App mailbox policy** window should appear that displays the Outlook Web App policy that was assigned to this mailbox. Verify the **OwaMailboxPolicy-Default** policy appears, and then select **Cancel**.
    - You will now assign the Outlook Web App mailbox policy that you created in the prior task to the mailboxes of three users who are participating in Adatum's pilot project.

      In the list of mailboxes, select **Diego Siciliani** and then hold down the CTRL key and select **Joni Sherman** and then **Patti Fernandez.**
7. By selecting multiple users, a **Bulk Edit** pane appears on the right side of the screen. Scroll down in this pane to the **Outlook on the web** section and then select **Assign a policy**.
8. In the **bulk assign Outlook Web App policy** window that opens, select **Browse.**
9. A window appears that displays the list of Outlook on the Web App Policies. Select the **Test OWA Mailbox policy** that you created in the prior task and then select **OK**.
10. In the **bulk assign Outlook Web App policy** window, select **Save** to apply this policy to all three user mailboxes.
11. Select **OK** once the information is successfully saved.
12. You should now verify the **Test OWA Mailbox policy** was applied to the users' mailboxes. You will use Joni's mailbox for this test. In the list of mailboxes, select **Joni Sherman**.
13. In the **Joni Sherman** detail pane on the right, scroll down to the bottom of the pane and in the **Email Connectivity** section, select **View details**.
14. An **Outlook Web App mailbox policy** window should appear that displays the Outlook Web App policy that was assigned to this mailbox. Recall in the earlier step that Joni was originally assigned the **OwaMailboxPolicy-Default** policy. You should now verify that Joni is assigned the **Test OWA Mailbox policy**. Select **Cancel**.
15. Leave the Edge browser and all tabs open and proceed to the next lab.

17 End of Lab 6

18 Module 8 – Lab 7 - Exercise 1 – Create Exchange Recipients

Adatum Corporation plans to create a hybrid Exchange deployment. They have Exchange Server 2019 and their on-premises user mailboxes installed on their on-premises Exchange Server (LON-EX1). Now that they are implementing Microsoft 365, they can also create user accounts and mailboxes in Exchange Online.

In your role as Holly Dickson, Adatum's Enterprise Administrator, you are interested in seeing how mailboxes are maintained in both Adatum's on-premises Exchange Server deployment as well as its new Microsoft 365 deployment. In the earlier lab on Implementing ActiveSync, you created on-premises user mailboxes for Holly, Paul Wimmer, and Jessica Hofer. Each mailbox was created in the on-premises **adatum.com** domain on LON-EX1. In this lab, you will create an Exchange Online user mailbox for Holly, which will be added to the **xxxxxZZZZZZ.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

18.1 Task 1 - Create a Cloud Recipient

In this task you will add a user account for Holly Dickson in Microsoft 365, which will create a mailbox for Holly in Exchange Online. In your role as Holly Dickson, you are still logged into Microsoft 365 as the MOD Administrator account. Holly will create this user account for herself, and she will assign herself the Exchange Admin role. You will perform this task in the LON-CL1 VM.

1. You should still be logged into LON-CL1 as the **Administrator** account with a password of **Pa55w.rd**; however, if the log-in screen appears, then log in now.
2. In your Edge browser, you should still have tabs open for the **Office 365 Home** page and the **Microsoft 365 admin center** tab from the prior lab. You should also be logged in as the MOD Administrator. If so, then proceed to the next step. However, if you closed your browser at the end of the prior lab, then navigate to the **Office 365 home** page, log in as **admin@xxxxxZZZZZZ.onmicrosoft.com,** and then navigate to the **Microsoft 365 admin center.**
3. In the **Microsoft 365 admin center**, select **Users** in the left-hand navigation pane, and then in the expanded group select **Active Users.**
4. In the **Active Users** window, note the 10 existing user accounts in the **Active Users** list. These accounts were added to Adatum's Microsoft 365 tenant by your lab hosting provider. Since Holly is not familiar with adding a new user in Microsoft 365, she wants to create a user account for herself.

   In the menu bar that appears above the list of active users, select **Add a user.** This initiates the **Add a user** wizard.
5. In the **Set up the basics** page, enter the following information:
   - First name: **Holly**
   - Last name: **Dickson**
   - Display name: When you tab into this field, **Holly Dickson** will appear.
   - Username: **Holly**

     IMPORTANT: To the right of the **Username** field is the domain field. It will be prefilled with the **xxxxxZZZZZZ.onmicrosoft.com** cloud domain (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

     After configuring this field, Holly's username should appear as: **Holly@xxxxxZZZZZZ.onmicrosoft.com**
   - Clear (uncheck) the **Automatically create a password**
   - Password: **Pa55w.rd**
   - Clear (uncheck) the **Require this user to change their password when they first sign in** check box
6. Select **Next**.
7. In the **Assign product licenses** page, enter the following information:
   - Select location: **United States**
   - Licenses: Under **Assign user a product license**, select **Office 365 E5**
8. Select **Next.**
9. In the **Optional settings** page, select the drop-down arrow to the right of **Roles (User: no administration access).**
10. In the **Roles information** that appears, select the **Admin center access** option. By doing so, the most commonly used Microsoft 365 administrator roles are displayed below this option and are available to be assigned.

    Note: All the admin roles will be displayed if you select **Show all by category**. For Holly, you do not need to view all the admin roles by category, since Holly will be assigned the Exchange Admin role that appears in this list of most commonly used roles. If you are interested in seeing what additional admin roles are available, select **Show all by category**.
11. In the list of most commonly used roles, select **Exchange Administrator** and then select **Next**.
12. On the **Review and finish** page, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.

13. On the **Holly Dickson added to active users** page, select **Show** that appears next to the string of asterisks for the **Password**. Verify that the password is **Pa55w.rd** and then select **Close.**

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

14. You should now see Holly Dickson's user account in the **Active users** list.

15. In the **Microsoft 365 admin center**, in the left-hand navigation bar, select **Show all** to display all the navigation menu options.

16. In the left-hand navigation pane, under the **Admin centers** group, select **Exchange**. This will open the EAC for Exchange Online in a new tab in your browser.

17. In the **Exchange Admin Center**, in the left-hand navigation pane, select **recipients.**

18. On the **recipients** page, the **mailboxes** tab is displayed by default. In the list of recipient mailboxes, you should see the Exchange Online mailbox that was automatically created for Holly when you created her Microsoft 365 user account.

19. Leave your Edge browser open and proceed to the next exercise.

19 Proceed to Lab 7 - Exercise 2

20 Module 8 - Lab 7 - Exercise 2 - Create Groups

In this exercise, you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. As part of her pilot project for deploying Microsoft 365, Holly wants to examine how creating groups in her on-premises Exchange Server 2019 environment differs from creating groups in Microsoft 365 for Exchange Online. You will begin by creating an on-premises distribution group for Exchange Server 2019 and then a cloud distribution group in Microsoft 365. You will finish by creating a Microsoft 365 group.

20.1 Task 1 - Create an On-premises Distribution Group

In this task you will log into the Exchange Server (LON-EX1) virtual machine and create an on-premises distribution group in the Exchange admin center for Exchange Server 2019.

1. Switch to **LON-EX1**, and if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.

2. In the **Edge** browser, you should still have the on-premises **Exchange admin center** open from a prior lab exercise; if so, then proceed to the next step. Otherwise, on the taskbar at the bottom of the page, select the **Start** icon, select the **Microsoft Exchange Server 2019** group in the menu, and in the drop-down list, select **Exchange Administrative Center**. Sign into the EAC as **adatum\Administrator** with a password of **Pa55w.rd**.

3. In the **Exchange admin center**, in the left-hand navigation pane, select **recipients**.

4. On the **recipients** page, select the **groups** tab at the top of the page.

5. Select the **plus (+) sign** icon on the menu bar to add a new group, and in the drop-down menu, select **Distribution group**.

6. In the **new distribution group** window, enter **Finance** in both the **Display name** and **Alias** fields.

7. Enter **This is the Finance team** in the **Notes** field.

8. Select the **Browse** button to the right of the **Organizational unit** field.

9. In the **select an organizational unit** window, select **Users** and then select **OK**.

10. Under the **Owners** field, note that the **Administrator** account, which you are signed in as, is automatically listed as an owner of this group. Since you want to add Holly Dickson as an additional owner for this group, select **plus (+) sign** icon.

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

12. In the **new distribution group** window, scroll down to the **Members** section. Since you are just adding the group now, there are no group members at this time.

However, verify that the **Add group owners as members** check box is selected so that Holly and the Administrator account, who are the two owners, will be automatically added as members of the group. Then select the **plus (+) sign** icon to add additional group members.

13. In the **Select Members** window, select **Jessica Hofer**, select the **add->** button, and then select **OK**.
14. This will be a Closed group, so in the two settings at the bottom of the page below the list of Members, select the **Closed** option for both the **Choose whether owner approval is required to join the group** setting and the **Choose whether the group is open to leave** setting.
15. Select **Save**.
16. On the **groups** page, the **Finance** distribution group should now appear in the list of groups.
17. Leave the Exchange admin center open and proceed to the next task.

20.2 Task 2 - Create a Cloud Distribution Group

Now that Holly has experienced adding a distribution group in Adatum's on-premises Exchange Server 2019 environment, she wants to add a distribution group in Microsoft 365. To avoid any confusion, Holly will switch to LON-CL1 to access the Exchange admin center for Exchange Online.

1. Switch to LON-CL1 and if necessary, log in as the **Administrator** with a password of **Pa55w.rd.**
2. In the Edge browser, you should still have the following tabs open from the prior lab exercise: the **Office 365 Home** tab, the **Microsoft 365 admin center** tab, and the **Exchange admin center** tab.

   Select the **Exchange admin center** tab, and in the left-hand navigation bar, select **New Exchange admin center**. You want to use the New Exchange admin center for managing distribution lists and groups.
3. On the **New Exchange admin** center, select **recipients** (if necessary) to expand the group, and then in the expanded group, select **Groups**.
4. On the **Groups** window, the **Microsoft 365** tab is displayed by default. Since you want to add a distribution group, select the **Distribution list** tab.
5. On the **Distribution list** tab, select **Add a group** on the menu bar. This initiates the **Add a group** wizard.
6. In the **Choose a group type** page, select the **Distribution** option and then select **Next**.
7. In the **Set up the basics** page, enter **Marketing** in the **Name** field, enter **This is the Marketing team** in the **Description** field, and then select **Next**.
8. In the **Edit settings** page, enter **Marketing** in the **Group email address** field.
9. This will be a Closed group, so select the **Closed** option for both the **Joining the group** setting and the **Leaving the group** setting, and then select **Next**.
10. In the **Review and finish adding group** page, review the current settings and if any need to be corrected, select the corresponding **Edit** option. When everything looks correct, select **Create group**.
11. On the **Marketing is created** page, select **Close**.

    Important: Note the message that appears at the top of this page. It can take up to an hour for the Marketing group to appear in your groups list.
12. On the **Groups** page, select **Refresh** on the menu bar to display the Marketing group in the list of distribution groups. Lab testing has indicated that this group typically appears within a few minutes, so select **Refresh** within 5 minutes to see whether the Marketing group appears.

    Note: You cannot continue until the Marketing group appears in this list of distribution groups.
13. Once the Marketing group appears in the list of distribution groups, select the **Marketing** group.
14. In the **Marketing** pane that appears, the **General** tab is displayed by default. Select the **Members** tab.

15. Under the **Owners** section, the **MOD Administrator** account is already displayed by default as an owner, since this is who you were logged in as in Microsoft 365 when you created the group.

    Below the MOD Administrator account, select **View all and manage owners**.

16. In the **Manage group owners** pane that appears, select in the **Add group owners** field. In the list of Microsoft 365 user accounts that appears, select **Holly Dickson**, and then select **Save changes**.

17. Select the back arrow in the upper left-hand corner of the **Manage group owners** pane to return to the **Marketing** pane.

18. On the **Members** tab, under the **Members** section, select **View all and manage members**.

19. In the **Manage group members** pane that appears, select in the **Add members** field. In the list of Microsoft 365 user accounts that appears, select **Joni Sherman**.

    Repeat this step to add **Megan Bowen** and **Nestor Wilke** as additional members of the group, and then select **Save changes**.

20. Select the X in the upper right-hand corner of the **Manage group members** pane to close it.

21. Leave your browser and all the tabs open and proceed to the next task.

20.3 Task 3 - Create a Microsoft 365 Group

In this task you will create a Microsoft 365 group, which is similar to an on-premises distribution group but with additional collaboration functionality. While email can be sent to each type of group, members of a distribution group receive email in their Inbox whenever someone sends an email to the email address associated with distribution group; whereas a Microsoft 365 group appears as an individual entity in Outlook and Outlook on the web if the user is a member of the Microsoft 365 group. Therefore, whenever an email is sent to a Microsoft 365 group, it does not land in the user's Inbox; rather, it lands in the separate group folder that is created in the user's mailbox in Outlook or Outlook on the web.

Another major difference between the two types of groups is that a Microsoft 365 Group is cloud-only and can be used for Team collaboration. Besides having a shared mailbox and calendar, a Microsoft 365 group can be created along with an associated SharePoint library, OneNote notebook, Microsoft Teams, Yammer, Planner, and PowerBI, all of which allows teams to seamlessly work together.

1. You should still be in the LON-CL1 VM; if necessary, log in as the **Administrator** account with a password of **Pa55w.rd**.

2. In your browser, if you have the **Microsoft 365 admin center** open in a tab from the previous task, then select this tab and proceed to the next step; otherwise, navigate to and sign in using the **Tenant Email** and **Password** provided by your lab hosting provider, and then navigate to the **Microsoft 365 admin center**.

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

4. In the **Active Groups** window, select **Add a group** on the menu bar. This initiates the **Add a group** wizard.

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

6. In the **Set up the basics** window, enter **Sales** in the **Name** field, and then enter **Collaboration group for the Sales team** in the **Description** field. Select **Next**.

7. In the **Assign owners** page, you will assign Allan Deyoung and Patti Fernandez as owners of this group.
    - Enter **Allan** in the **Owners** field. In the drop-down menu that appears, select **Allan Deyoung**.
    - Enter **Patti** in the **Owners** field. In the drop-down menu that appears, select **Patti Fernandez**.
    - Select **Next**.

8. In the **Edit settings** page, enter **sales** in the **Group email address** field.

9. Under the **Privacy** section, select the **Private – Only members can see group content** option.

10. Under the **Add Microsoft Teams to your group** section, verify the **Create a team for this group** check box is selected (select it if need be).

11. Select **Next**.
12. In the **Review and finish adding group** page, review the content that you entered. If everything is correct, select **Create group**; otherwise, select **Back** and fix anything that needs correction (or select **Edit** under the specific area that needs adjustment).
13. On the **New group created** page, note the comment at the top of the page that it may take 5 minutes for the new group to appear in the list of groups.

    Select **Close**. This returns you to the **Groups** page.
14. If the new Sales group does not appear in the **Groups** list, wait a minute or so and then select **Refresh** on the menu bar. If the Sales group still does not appear, then refresh the page every minute or so until it does.

    Note: Two additional group types are Mail-enabled Security groups and Distribution groups. Neither of these group types were used in this lab because it can take up to an hour for these two types of groups to appear in the Groups list; whereas Microsoft 365 groups and Security groups usually take just a matter of minutes to appear.
15. You're now ready to add members to the Sales group. In the list of **Active groups**, select the **Sales** group.
16. In the **Sales** pane that appears, the **General** tab is displayed by default. Select the **Members** tab.
17. Under the **Owners** section, you can see the two owners (Allan and Patti), but you can also see that there are no members. Under the **Members** section, select **View all and manage members** to add members to the group.
18. In the **Sales** group window, select **+ Add members**. This displays the list of current Microsoft 365 users.
19. In the list of users, select the check boxes for **Diego Siciliani** and **Lynne Robbins**, and then scroll to the bottom and select **Save**.
20. In the **Sales** window, select **Close**. This displays the list of users for this group. Select **Close** again.
21. On the **Sales** window, Diego and Lynne should now appear as members of the group. If they do not appear, select the **Refresh** icon in the upper right-hand corner of the screen.

    Once Lynn and Diego appear as members of the group, select the **X** in the upper right-hand corner to close the window.
22. On the **Active groups** window, note the difference between the **Marketing** distribution list that you added in the prior task and the **Sales** group that you added in this task.

    Under the **Teams status** column, note the Sales group displays an icon indicating the group is connected to Microsoft Teams (hover your mouse over the icon to see the icon tag). However, the Marketing distribution list, which was added through the Exchange admin center for Exchange Online, does not display this icon. This is because the EAC does not provide this Teams option when adding a group through the EAC.

    To further elaborate on this difference, select the **Sales** group in the list of groups.
23. In the **Sales** group window that appears, note the four tabs that appear at the top – General, Members, Settings, and Microsoft Teams. Select the **Microsoft Teams** tab.
24. In the **Microsoft Teams** tab, note that you have the option to navigate to the **Microsoft Teams admin center** to manage your Teams settings. Select the **X** in the upper right-hand corner of the **Sales** window to close it.
25. In the **Active groups** window, select the **Marketing** group.
26. In the **Marketing** group window, note that a **Microsoft Teams** tab does not appear. This is because when you added the group through the EAC, it did not provide an option to create a team for this group in Microsoft Teams.

    Select the **X** in the upper right-hand corner of the **Marketing** window to close it.
27. Leave your browser and all the tabs open for the next exercise.

21 End of Lab 7

22 Module 9 - Lab 8 - Exercise 1 - Create Public Folders

Holly Dickson wants to continue reviewing the messaging functionality in Microsoft 365, and more specifically, the use of public folders. In this lab, you will log into the Exchange admin center for Exchange Online and create a public folder mailbox and a public folder in Microsoft 365.

Public folder mailboxes contain the hierarchy information plus the content for public folders. The first public folder mailbox you create will be the primary hierarchy mailbox, which contains the only writable copy of the hierarchy. Any additional public folder mailboxes you create will be secondary mailboxes, which contain a read-only copy of the hierarchy.

Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. You can't create a public folder unless you've first created a public folder mailbox.

22.1 Task 1 - Create a Public Folder Mailbox

In this task, you will create a public folder mailbox as part of Holly's Microsoft 365 pilot project. Every public folder must be contained in a public folder mailbox; therefore, you must create the public folder mailbox first before you can create a public folder.

1. You should still be logged into LON-CL1 from the prior lab; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In the Edge browser, the Office 365 home page, the Microsoft 365 admin center, and the Exchange admin center tabs should still be open. Select the **Exchange admin center** tab (if you have both the classic EAC and the New EAC open, select the classic EAC; public folders have not yet been added to the New EAC).
3. In the **Exchange admin center**, on the left-hand navigation pane, select **public folders**.
4. At the top of the **public folders** page, select the **public folder mailboxes** tab.
5. On the **public folder mailboxes** tab, select the **plus (+) sign** icon on the menu bar to add a new public folder mailbox.
6. In the **new public folder mailbox** window, enter **Test PF mailbox1** in the **Name** field, select **Save**, and then select **OK** once the information is successfully saved.
7. This will return you to the **public folder mailboxes** list, which should now display **Test PF mailbox1**.
8. Leave all browser tabs open and proceed to the next task.

22.2 Task 2 - Create a Public Folder

Now that you have created a public folder mailbox, you can create a public folder. When using the EAC to create a public folder, you'll only be able to set the name and the path of the public folder. To configure additional settings, you'll need to edit the public folder after it's created (which you will do in the next lab exercise).

1. You should still be in LON-CL1 and you should be in the **Exchange admin center** tab in your browser.
2. In the **Exchange admin center**, you should still be in the **public folders** page, and you should be in the **public folder mailboxes** tab after having completed the prior task.

   Since you now want to create a public folder, select the **public folders** tab at the top of the page.
3. In the **public folders** tab, select the **plus (+) sign** icon to add a new public folder.
4. In the **new public folder** window, enter **Test PF1** in the **Name** field, select **Save,** and then select **OK** once the information is successfully saved.
5. This will return you to the **public folder** list, which should now display **Test PF1**.
6. Leave all browser tabs open and proceed to the next lab exercise, where you will enable mail settings for this **Test PF1** public folder.

23 Proceed to Lab 8 - Exercise 2

24 Module 9 - Lab 8 - Exercise 2 - Manage Public Folders

In the prior exercise, Holly Dickson logged into the Exchange admin center for Exchange Online on LON-CL1 and created a Microsoft 365 public folder mailbox and a public folder. In this exercise, she will manage settings and permissions for each of these objects using the Exchange Online EAC.

24.1 Task 1 - Manage Public Folder Mail Settings

In this task, you will continue in your role as Holly Dickson and enable the Test PF1 public folder that you created in the prior exercise so that it can receive email.

1. You should still be logged into LON-CL1 from the prior lab; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In the Edge browser, you should still be in the **Exchange admin center** from the end of the prior task. Specifically, you should still be on the **public folders** page, and you should be in the **public folders** tab.
3. On the **public folders** page, the **Test PF1** record that you created in the prior task should be highlighted.

   Important: If you closed the EAC tab at the end of the prior task and had to navigate to this page in the prior step, then select the **Test PF1** row. Do not select the **Test PF1** hyperlink as this will open the **Test PF1** public folder window. Instead, select any other portion of the **Test PF1** row to simply highlight the record.
4. By selecting the Test PF1 record, the properties for this public folder are displayed in the detail pane on the right. Note the current **Mail settings** for Test PF1 is set to Disabled. To enable mail for this public folder, select **Enable**.
5. A **Warning** dialog box will appear that asks whether you want to enable email for the selected public folders. Select **Yes**.
6. In the detail pane on the right, the **Mail settings** should now be **Enabled.**
7. Leave all browser tabs open and proceed to the next task.

24.2 Task 2 - Manage Public Folder Settings

In this task, you will manage several settings for the Test PF1 public folder.

1. You should still be in LON-CL1 and you should be in the **Exchange admin center** tab in your browser.
2. In the **Exchange admin center**, you should still be in the **public folders** page, and you should be in the **public folders** tab after having completed the prior task.
3. On the **public folders** page, the **Test PF1** record that you updated in the prior task should be highlighted.

   Important: If you closed the EAC tab at the end of the prior task and had to navigate to this page in the prior step, then select the **Test PF1** row. Do not select the **Test PF1** hyperlink as this will open the **Test PF1** public folder window. Instead, select any other portion of the **Test PF1** row to simply highlight the record.
4. With the **Test PF1** record highlighted in the public folder list, select the **pencil (Edit)** icon in the menu bar to edit the record. This opens the **Test PF1** properties window.
5. In the **Test PF1** properties window, the **general** tab in the left-hand navigation pane is displayed by default. Review the fields in this tab and note the value in the **Public folder mailbox** field; this indicates that **Test PF1** was automatically assigned to the **Test PF mailbox1** that you created in the first task in this exercise.
6. In the **Test PF1** properties window, in the left-hand navigation pane, select the **general mail properties** tab.
7. Change the value of the **Display Name** field to **First public folder.**

8. Select the **Hide from Exchange address list** checkbox.

   Note: By selecting this check box, the public folder will not appear in Adatum's address book and other address lists, but it will still receive email.

9. In the left-hand navigation pane, select the **mail flow settings** tab.
10. Under the **Display Name** field, select the **Require that all senders are authenticated** check box.
11. Select **Save**. Once the settings have been saved, select **Close**.
12. Leave all browser tabs open and proceed to the next task.

24.3 Task 3 - Manage Public Folder Permissions

In this task, you will manage the permissions for the Test PF1 public folder.

1. You should still be in LON-CL1 and you should be in the **Exchange admin center** tab in your browser.
2. In the **Exchange admin center**, you should still be in the **public folders** page, and you should be in the **public folders** tab after having completed the prior task.
3. On the **public folders** page, the **Test PF1** record that you updated in the prior task should be highlighted.
4. With the **Test PF1** record highlighted in the public folder list, a **Test PF1** detail pane will be displayed on the right side of the screen. In the detail pane, under **Folder permissions**, select **Manage**.
5. A **Test PF1** window will appear that enables you to add or remove users who can access this public folder and edit its permissions. Select the **plus (+) sign** icon to add users.
6. In the **public folder permissions** window, select the **Browse** button to the right of the **User** field, select **Holly Dickson,** and then select **OK**.
7. Select the drop-down arrow in the **Permission level** field and select **Owner.**
8. Select **Save** at the bottom of the **public folder permissions** window.
9. Select **Save** at the bottom of the **Test PF1** window. Once the settings have been saved, select **Close**.
10. Leave all browser tabs open and proceed to the next lab.

25 End of Lab 8

26 Module 10 - Lab 9 - Exercise 1 - Prepare Azure AD for Hybrid Synchronization

In this lab you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Adatum has decided to transition from their current Microsoft Exchange on-premises deployment to a hybrid deployment that utilizes Exchange Online within Microsoft 365. Adatum's CTO has tasked you with implementing this hybrid deployment. In this lab, you will perform the tasks necessary to prepare your messaging environment for your eventual hybrid deployment.

To complete this task, you must first prepare Azure Active Directory to support the hybrid synchronization between Exchange on-premises and Exchange Online. This will require that you:

- Configure your lab environment to support local mail transport
- Add an accepted domain to your Azure AD forest
- Configure the UPN Name for the new domain
- Configure Exchange to use the new domain
- Enable directory synchronization by installing and running the Microsoft Azure Active Directory Connect tool
- Perform a Full Synchronization to migrate Adatum's on-premises user accounts to the new domain in Microsoft 365

While your trial tenant has already been set up by your lab hosting provider, you must ensure that your local, on-premises Active Directory is ready for hybrid synchronization before you create your hybrid deployment. You will do this by adding a custom, accepted domain to the Azure Active Directory forest and then configure Exchange to use the new accepted domain.

Once you finish configuring Azure AD for hybrid synchronization in this lab, you will then set up Exchange for a hybrid deployment and then test your new deployment.

26.1 Task 1: Configure your tenant to support local mail transport

Before you begin setting up Adatum's hybrid deployment, you must first configure your hosted lab environment to support local mail transport.

IMPORTANT: The steps that you perform in this task are NOT required to set up a hybrid environment in a real-world scenario. Instead, they must be performed to configure the hosted virtual machines used in this training lab so that email can be sent locally between on-premises and cloud users when testing your hybrid deployment.

1. Switch to **LON-EX1** and if necessary, log in as the **Administrator** account with a password of **Pa55w.rd**.
2. If your Edge browser is still open from Lab 1, then minimize the browser now (do not close it).
3. You need to open the **Network and Sharing Center**. To do so, select the network icon on the right-side of the system tray at the bottom of the screen (which displays **Adatum.com Internet access**), and in the menu that appears, select **Network & Internet settings**.
4. In the **Settings** window, scroll to the bottom of the **Status** pane on the right and select **Network and Sharing Center**.
5. In the **Network and Sharing Center**, under the **View your active networks** group, select **Ethernet** (which appears to the right of **Connections**:).
6. In the **Ethernet Status** window, select the **Properties** button that appears at the bottom of the window.
7. In the **Ethernet Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** and then select the **Properties** button.

   WARNING: Do NOT select the check box for **Internet Protocol Version 4 (TCP/IPv4)**, which will uncheck it. This check box MUST remain checked. Simply select this item to highlight it so that you can update its properties.
8. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window is already set up to use an existing IP address. Since you are going to add an additional IP address, select the **Advanced** button in the bottom-right corner of the screen.
9. In the **Advanced TCP/IP Settings** window, in the **IP Settings** tab, it displays two groups: **IP addresses** and **Default gateways**.

   Under the **IP addresses** group, select the **Add...** button.
10. A **TCP/IP Address** pop-up window is displayed. Enter **10.0.0.6** in the **IP address** field, enter **255.255.255.0** in the **Subnet mask** field, and then select **Add**.

    NOTE: If you enter the IP address or subnet mask incorrectly, you will receive an error when selecting **Add**. If this occurs, you must close the window and then reopen it before entering the correct values. If you do not close the window and reopen it, you will still receive the error even if you enter the values correctly.
11. In the **Advanced TCP/IP Settings** window, it should now display **10.0.0.6** as a supported IP address, with a subnet mask of **255.255.255.0**. Select **OK**.
12. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, select **OK**.
13. In the **Ethernet Properties** window, select **Close**.
14. In the **Ethernet Status** window, select **Close**.
15. Close the **Network and Sharing Center** window.

16. Close the **Settings** window.

26.2 Task 2: Create a Custom Domain in Microsoft 365

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

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

Most companies do not personally manage their domains' DNS records themselves; instead, they have a third-party resource that manages these records for them. To assist in this effort, Microsoft 365 provides certain third-party domain registrars with an automation tool that automatically adds and replaces a company's DNS records. The automation tool also federates the sign in credentials for the third-party registrars and Microsoft 365. Using a tool to automatically maintain DNS records is a much-welcomed improvement from the days when companies had to manually maintain these records, which oftentimes introduced human error into a rather complicated process. Because these tools eliminate the need to manually add the DNS records, they eliminate human error from the process.

That being said, for the purpose of this lab, you will be asked to manually create the necessary DNS records required by this new custom domain. In the other Microsoft 365 training courses that use a custom domain (such as MS-101T00 and MS-030T00), the custom domain and its DNS records will be added into Adatum's Microsoft 365 deployment by the lab hosting provider, who will take on the role of the third-party domain registrar for Adatum. However, this MS-203T00 training course will task you with adding the domain and creating its required DNS records so that you gain experience and understanding of what the DNS records are about and why they are required for a new domain.

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

1. Switch to **LON-DC1** and, if necessary, log in as **Administrator** and password **Pa55w.rd**.
2. You must now open **Windows PowerShell**. Select the magnifying glass (Search) icon on the taskbar at the bottom of the screen and type **powershell** in the Search box that appears.

   In the list of search results, right-click on **Windows PowerShell** (do not select Windows PowerShell ISE) and select **Run as administrator** in the drop-down menu that appears. Maximize your PowerShell window.
3. At the command prompt, you should run the following command to create a new zone in your on-premises DNS:

   IMPORTANT: Before you run the following command, remember to replace **xxxUPNxxx** with the unique UPN name assigned to your tenant by your lab hosting provider, and replace **xxxCustomDomainxxx.xxx** with your lab hosting provider's custom domain name:

   ```
   dnscmd /zoneadd xxxUPNxxx.xxxCustomDomainxxx.xxx /DsPrimary
   ```
4. Minimize your Windows PowerShell window (do NOT close it as you will use it later).
5. You will now access the **Microsoft 365 admin center** from LON-DC1. Select the **Microsoft Edge** icon on your taskbar and enter the following URL in the address bar: **https://portal.office.com.**
6. On the **Sign in** page, enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider), and then enter the tenant email password provided by your lab hosting provider on the **Enter password** page. Select **Sign in.**

7. On the **Stay signed in?** window, select the **Don't show this again** check box and then select **Yes.**
8. If a **Get your work done with Office 365** window appears, select the **X** in the upper right-hand corner to close it.
9. In the **Office 365 home** page, in the column of Microsoft 365 app icons on the left-side of the screen, select the **Admin** icon to navigate to the **Microsoft 365 admin center**.
10. In the **Microsoft 365 admin center**, in the left-hand navigation bar, select **Show all,** select **Settings**, and then under the **Settings** group select **Domains**.
11. On the **Domains** page, note that in the list of domains, only the **xxxxxZZZZZZ.onmicrosoft.com** domain appears. The existing on-premises **adatum.com** domain does not appear in the list of Microsoft 365 domains.

    To add Adatum's new Microsoft 365 domain, select **+Add domain** in the menu bar that appears above the list of domains; this will start the **Add domain** wizard.
12. In the **Add a domain** page, in the **Domain name** field, enter your domain name in the form of **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx is the unique UPN name provided by your lab hosting provider, and xxxCustomDomainxxx.xxx is your lab hosting provider's domain name), and then select the **Use this domain** button at the bottom of the page.
13. In the **How do you want to verify your domain?** page, you must select a verification method to prove you own the domain. For this lab, select the **Add a TXT record to the domain's DNS records** option and then select **Continue**.
14. On the **Verify you own this domain** page, you must copy the **TXT value** (NOT the TXT name) so that you can configure the domain later on in DNS Manager.

    To do so, select the **Copy record** icon that appears to the left of the **TXT value** (to the left of **MS=msXXXXXXXX**). If a dialog box appears, select **Allow access** to copy this value from the webpage to your clipboard.

    Important: Do NOT select the **Verify** button at this point; **instead, proceed to the next step.** However, if you did select the **Verify** button, you will receive an error indicating the system could not find the record you added for this domain (you can do this if you want to see the error; there is no harm in it). Therefore, you must complete the next series of steps to add the TXT record to this domain in **DNS Manager**. Once you finish that process, you will be instructed to return to this page and select the **Verify** button so that you can complete the process of adding this domain in the Microsoft 365 admin center.
15. Before you can verify you own this domain in the **Add domain** wizard, you must first add a DNS record for this domain in Server Manager. Select the **Server Manager** icon that appears in your taskbar at the bottom of the page. Maximize the Server Manager window if necessary.
16. In **Server Manager Dashboard,** select **Tools** in the top right corner of the window. In the drop-down menu that appears, select **DNS**, which will open **DNS Manager**. Maximize the DNS Manager window.
17. In the **DNS Manager** window, in the **File Explorer** section in the left-hand column, under **LON-DC1** expand the **Forward Lookup Zones** folder and then select the **xxxUPNxxx.xxxCustomDomainxxx.xxx** zone that you previously added in Windows PowerShell (where xxxUPNxxx is the unique UPN name provided by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's domain name).
18. Right-click on this **xxxUPNxxx.xxxCustomDomainxxx.xxx** zone, and in the menu that appears, select **Other New Records...**
19. In the **Resource Record Type** window that appears, in the **Select a resource record type** field, scroll down and select **Text (TXT),** and then select the **Create Record...** button at the bottom of the window.
20. In the **New Resource Record** box, in the **Text (TXT)** tab, leave the **Record name** field blank. However, right-click in the **Text** field and select **Paste** from the menu that appears. This will paste in the TXT valued of **MS=msXXXXXXXX** that you copied to the clipboard when you were in the Microsoft 365 admin center.
21. Select **OK** to create the record.

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

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

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

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

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

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

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

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

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

26. In the **Add DNS records** window, it enables you to add DNS records for three services that DNS supports - Exchange and Exchange Online Protection, Skype for Business, and Intune and Mobile Device Management for Microsoft 365. **Exchange and Exchange Online Protection** is displayed by default and its check box is also selected by default.

    To see the other two services, select **Advanced Options**. Note that under **Advanced Options**, neither the **Skype for Business** nor the **Intune and Mobile Device Management for Microsoft 365** check boxes are selected.

    Important: Only the **Exchange and Exchange Online Protection** check box should be selected for the purpose of this lab; this is sufficient for Adatum.

    Do NOT select either of the other two check boxes. We had you select **Advanced Options** just to see where you would select these other two services in the event you would need to do so in your real-world deployment.

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

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

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

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

- In the **MX Records** section, under the **Points to address or value** column, select the copy icon that appears to the left of the expected value (for example, **xxxUPNxxx-xxxCustomDomainxxx-xxx.mail.protection.outlook.com**) to copy this value to the clipboard. If a dialog box appears, select **Allow access** to allow the webpage to copy the value to the clipboard.
- You must now switch to DNS Manager. On the taskbar at the bottom of the page, select the **DNS Manager** icon.
- In **DNS Manager**, under **Forward Lookup Zones**, the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain should be selected from when you earlier left off. If not, select this zone now. You should see the **TXT** record that you created earlier. You must now create a **Mail Exchanger (MX)** record for this domain.

  Under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Mail Exchanger (MX)...**
- In the **New Resource Record** window, in the **Mail Exchanger (MX)** tab, leave the **Host or child domain** field blank, but right-click in the **Fully qualified domain name (FQDN) of mail server** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you just copied to the clipboard.
- Select **OK**. Note how this Mail Exchanger (MX) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.
- Switch back to the **Add DNS records** page in the Microsoft 365 admin center by selecting the **Microsoft Edge** icon on the taskbar at the bottom of the page. At this point, you can either select **Continue** at the bottom of the **Add DNS records** page to verify the MX record that you just added, or you can wait until you have added all three records and then select **Continue** to verify all three records at once.

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

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

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

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

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

      Therefore, the only value you need to copy for the CNAME record is the expected value for the **Points to address or value** column (for example, autodiscover.outlook.com).
    - On the taskbar at the bottom of the page, select the **DNS Manager** icon.
    - In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **New Alias (CNAME)...**

- In the **New Resource Record** window, enter **autodiscover** in the **Alias name (uses parent domain if left blank)** field.
- Right-click in the **Fully qualified domain name (FQDN) for target host** field and select **Paste** from the menu that appears. This will paste in the expected **Points to address or value** that you earlier copied to the clipboard.
- Select **OK**. Note how this Alias (CNAME) record appears in the details pane on the right for the xxxUPNxxx.xxxCustomDomainxxx.xxx domain that you previously created. Leave your DNS Manager window open as you will return to it in a later step in this task.
- Switch back to the **Add DNS records** page in the Microsoft 365 admin center. On the taskbar at the bottom of the page, select the **Microsoft Edge** icon and select the **Microsoft 365 admin center** tab. At this point, you can either select **Continue** at the bottom of the **Add DNS records** page to verify the CNAME record, or you can wait until you have added all three records and then select **Continue** to verify all three records at once.

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

30. Once a check mark appears next to **CNAME Records**, you will finish by adding the **TXT record** required by Exchange and Exchange Online Protection service.
    - On the **Add DNS records** page, in the **TXT Records** section, under the **TXT value** column, select the copy icon that appears to the left of the expected value (for example, **v=spf1 include:spf.protection.outlook.com -all**) to copy this value to the clipboard.
    - On the taskbar at the bottom of the page, select the **DNS Manager** icon.
    - In **DNS Manager**, under **Forward Lookup Zones**, right-click the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain and select **Other New Records...**
    - In the **Resource Record Type** window that appears, in the **Select a resource record type** field, scroll down and select **Text (TXT),** and then select the **Create Record...** button at the bottom of the window.
    - In the **New Resource Record** window, in the **Text (TXT)** tab, leave the **Record name** field blank. However, right-click in the **Text** field and select **Paste** from the menu that appears. This will paste in the expected **TXT value** that you earlier copied to the clipboard.
    - Select **OK**.
    - On the **Resource Record Type** window, select **Done**.
31. In **DNS Manager**, you should now see the TXT record that you originally created to verify the domain, along with the MX, CNAME, and TXT records that you created for the Exchange service to work within this domain.

    Minimize the DNS Manager window.
32. This should return you to the **Add DNS records** window in your Edge browser. Select **Continue** to complete the new domain setup. If you selected **Continue** after adding the MX and CNAME records, and if each validated successfully, then only the TXT record will be validated at this point. However, if you did not select **Continue** after adding the MX and CNAME records, then all three records will be validated at this point.
    - If all three records have been successfully validated, then the **Domain setup is complete** page will appear. If this occurs, then select the **Done** button to complete the domain setup process.
    - However, if any of the three records did not validate successfully, then the **Add DNS records** window will return, and it will display either a check mark or an exclamation point next to each record type to indicate which ones validated successfully and which ones did not. An exclamation point in a red circle indicates that there was a problem with the record, and it did not validate successfully (note that the Actual value for the record is left blank). If this occurs, you must correct the data on the corresponding record in DNS Manager and then select **Continue** again. You must

repeat this process until all three records have successfully validated and the **Domain setup is complete** page appears.

33. Once the domain setup process is complete and the three DNS records validated successfully for the **Exchange and Exchange Online Protection** service, the **Domains** page will be displayed. Verify the **Domain status** for your new domain is **Healthy**.

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

26.3 Task 3: Configure the UPN name for custom domain

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

If you recall, your VM environment was created by your lab hosting provider with an on-premises domain titled **adatum.com**. This domain included several on-premises user accounts, such as Holly Spencer, Laura Atkins, and so on. Then in the prior task, you created a custom, accepted domain for Adatum titled **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx was the unique UPN name assigned to your tenant, and xxxCustomDomainxxx.xxx was the name of your lab hosting provider's custom domain).

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

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

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

1. You should still be logged into LON-DC1 as the **Administrator** with a password of **Pa55w.rd**; if necessary, log in now.

2. In this task, you will run two PowerShell commands. To save you from having to manually type in the commands (which are quite lengthy) into PowerShell, you will copy the commands from these instructions and then paste them into Notepad. You will then use the "Replace" functionality in Notepad to find and replace the custom domain name placeholder in the commands with the actual domain name, and then you will copy and paste each command from Notepad into PowerShell.

   Select the **magnifying glass (Search)** icon on the taskbar and then enter **note** in the Search field. In the menu that appears, select **Notepad**. Maximize the Notepad window once it opens.

3. While the PowerShell commands that you need to run are provided in steps 7 and 8, it will be easier to copy these steps into Notepad, perform a **Replace** command to replace the custom domain name parameter with your actual new domain name, and then copy the commands in Notepad and paste them into PowerShell. This will save you from having to enter some lengthy PowerShell commands.

   Therefore, copy the PowerShell commands from **steps 7 and 8** below and paste them into Notepad.

   Hint: To simplify this process, copy all the text for steps 7 and 8 and not just the PowerShell commands; that way you can do one Copy statement rather than two Copy statements of just the PowerShell commands.

4. Once you have copied steps 7 and 8 into Notepad, select **Edit** on the Notepad menu bar and then select **Replace**.

5. In the **Replace** window, copy **xxxUPNxxx.xxxCustomDomainxxx.xxx** and paste it into the **Find what** field. In the **Replace with** field, enter the new domain you previously added, select **Replace all**,

and then close the **Replace** window.

Important: Review the Notepad document and verify that both commands were updated by replacing **xxxUPNxxx.xxxCustomDomainxxx.xxx** with the new accepted domain name. Verify you spelled the new domain name correctly.

6. If **Windows PowerShell** is still open, then select the **Windows PowerShell** icon on your taskbar; otherwise, you must open and elevated instance of **Windows PowerShell** just as you did earlier (remember to **Run as administrator)**.
7. You will now begin the process of copying each of the PowerShell commands (from this step through step 8) from Notepad and pasting them one at a time into Windows PowerShell and then running them.

   In the following PowerShell command, the **Set-ADForest** cmdlet modifies the properties of an Active Directory forest, and the **-identity** parameter specifies the Active Directory forest to modify.

   Select the **Notepad** icon on the taskbar and then copy the following command from Notepad (select the command, right-click on it, and then select **Copy**), paste it into PowerShell at the command prompt (right click on the command prompt and select **Paste**), and then hit ENTER to run it.

   Note: Traditionally, you must right-click at the command prompt, select Paste, and then hit ENTER on the keyboard to run a command. However, in some VM environments, you just have to right-click at the command prompt to both paste in the copied command AND run it.

   Set-ADForest -identity adatum.com -UPNSuffixes @{replace="xxxUPNxxx.xxxCustomDomainxxx.xxx"}
8. Copy the following command from Notepad, paste it into PowerShell at the command prompt, and then run it.

   This command changes all existing adatum.com accounts to the new UPN @xxxUPNxxx.xxxCustomDomainxxx.xxx domain:

   Get-ADUser -Filter * -Properties SamAccountName | ForEach-Object { Set-ADUser $_ -UserPrincipalName ($_.SamAccountName + "@xxxUPNxxx.xxxCustomDomainxxx.xxx")}
9. Wait for PowerShell to complete the prior command and return to the command prompt, and then close the Windows PowerShell window.
10. Close Notepad (do not save the untitled document).
11. Leave the Edge browser and all tabs open and proceed to the next task.

26.4 Task 4: Enable Exchange for the Custom Domain

In this task, you will log into the on-premises Exchange Server (LON-EX1) VM and enable your Exchange on-premises environment for the accepted domain (**xxxUPNxxx.xxxCustomDomainxxx.xxx**) that you added and configured in the prior tasks. You will run a series of PowerShell commands in the Exchange Management Shell, and you will update additional settings in the on-premises Exchange Admin Center. In the prior task, you ran the PowerShell commands in Windows PowerShell on LON-DC1. In this task, you will run Exchange-specific PowerShell commands on LON-EX1; therefore, you will use the Exchange Management Shell rather than Windows PowerShell.

To save you from having to manually type in the commands (which are quite lengthy) into the Exchange Management Shell, you will copy the commands from these instructions and then paste them into Notepad, just as you did in the prior task. You will then use the "Replace" functionality in Notepad to find and replace the custom domain name placeholder in the commands with the actual domain name, and then you will copy and paste each command from Notepad into the Exchange Management Shell.

1. Switch to **LON-EX1** and, if necessary, log in as the **Administrator** with a password of **Pa55w.rd**. If you had to log in and the **Server Manager** application automatically opened, then close it now.
2. In this task, you will enter a series of Exchange-specific PowerShell commands through the **Exchange Management Shell**. These commands will enable your on-premises Exchange environment for the new **xxxUPNxxx.xxxCustomDomainxxx.xxx** accepted domain.

   To expedite running these commands, open **Notepad** just as you did in the prior task, maximize the

Notepad window, and then copy **steps 5-15** below and paste them into the Notepad document (to make it easy, copy all the text for steps 5-15 and not just the PowerShell commands; that way you can do one Copy statement rather than 11 Copy statements of just the PowerShell commands).

Warning: Some lab hosting providers' VM environments limit the amount of text that can be copy and pasted at one time into a VM. If this occurs within your VM environment, you may have to copy and paste steps 5-15 in chunks to get all 11 steps copied into Notepad.

3. In the prior task, after you copied the two steps into Notepad, you did one mass replace on xxxUPNxxx.xxxCustomDomainxxx.xxx. However, in this task, one of the commands just references xxxCustomDomainxxx.xxx and not the xxxUPNxxx UPN name, so in this task, you should replace each portion of the domain name separately.

   After copying the commands from steps 5-15 into Notepad, perform the following two (2) **Replace** commands in Notepad:

   - Replace all instances of **xxxUPNxxx** with the **UPN Name** provided by your lab hosting provider.
   - Replace all instances of **xxxCustomDomainxxx.xxx** with the accepted domain provided by your lab hosting provider.
   - **Important:** Review the Notepad document and verify that all instances of xxxUPNxxx have been replaced with your UPN Name, and all instances of xxxCustomDomainxxxx.xxx have been replaced with your new domain name.
   - Close the **Replace** window.

4. To open the **Exchange Management Shell**, select the Windows icon on the bottom left corner of the taskbar, and then in the menu select **Microsoft Exchange Server 2019** to expand this program group, and then in the group, select **Exchange Management Shell**.

   Maximize the **Exchange Management Shell** window once it opens. Wait for the command prompt to appear before proceeding.

5. You will now begin the process of copying each of the PowerShell commands in Notepad and then pasting and running them in the Exchange Management Shell.

   Select the **Notepad** icon on the taskbar, and in your Notepad document, start with this Step 5.

   Select the following PowerShell command from step 5 in the Notepad document, right-click on it, and select **Copy**, paste it into the Exchange Management Shell at the command prompt (right click on the command prompt and select **Paste;** Note – in some VM environments, just right-clicking at the command prompt will paste in the copied command), and then press Enter on your keyboard.

   This command will add a new send connector with a wildcard (asterisk) to accept all emails from any domain:

   New-SendConnector -Name "To Internet" -AddressSpaces "*"

6. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will add the accepted xxxUPNxxx.xxxCustomDomainxxx.xxx domain as a Micro, set it as a trusted domain, and assign it the Alias of A.Datum:

   New-AcceptedDomain -DomainName "xxxUPNxxx.xxxCustomDomainxxx.xxx" -DomainType Authoritative -Name "A.Datum"

7. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the default email policy for every user to have its primary email address as the accepted domain of xxxUPNxxx.xxxCustomDomainxxx.xxx:

   Set-EmailAddressPolicy -Identity "Default Policy" -EnabledPrimarySMTPAddressTemplate "SMTP:%m@xxxUPNxxx.xxxCustomDomainxxx.xxx"

8. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will update the default email policy that was just changed in the previous command:

   Update-EmailAddressPolicy -Identity "Default Policy"

9. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the OWA Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OWA:

   Set-OwaVirtualDirectory -Identity "LON-EX1\OWA (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustom -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OWA

   NOTE: Ignore the warning that's displayed. This warning is addressed when you run the next command.

10. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the ECP Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ECP:

    Set-EcpVirtualDirectory -Identity "LON-EX1\ECP (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustomD -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ECP

11. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Active Sync Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync:

    Set-ActivesyncVirtualDirectory -Identity "LON-EX1\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/Microsoft-Server-Activesync

12. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Web Services Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ews/exchange.asmx:

    Set-WebServicesVirtualDirectory -Identity "LON-EX1\EWS (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/ews/exchange.asmx -InternalUrl https://xxxUPNxxx.xxxCustomDom

    NOTE: This command takes a little time to process once you hit Enter. After several seconds (possibly up to 10-20 seconds), you will receive a prompt that indicates the InternalURL parameter can't be resolved. At the prompt, enter **A** for **Yes to All** to continue and then press **Enter**.

13. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the OAB Virtual Directory to https://xxxUPNxxx.xxxCustomDomainxxx.xxx /OAB:

    Set-OabVirtualDirectory -Identity "LON-EX1\OAB (Default Web Site)" -ExternalUrl https://xxxUPNxxx.xxxCustom -InternalUrl https://xxxUPNxxx.xxxCustomDomainxxx.xxx/OAB

14. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the internal and external address for the Outlook Anywhere external host name to xxxUPNxxx.xxxCustomDomainxxx.xxx and to set the authentication method to NTLM and to require external clients to use SSL to make the connection:

    Set-OutlookAnywhere -Identity "LON-EX1\Rpc (Default Web Site)" -ExternalHostname xxxUPNxxx.xxxCustomDomainxxx.xxx -ExternalClientsRequireSsl $true -ExternalClientAuthenticationMethod NTLM -InternalHostname xxxUPNxxx.xxxCustomDomainxxx.xxx -InternalClientsRequireSsl $true -InternalClientAuthenticationMethod NTLM

15. Copy the following command from Notepad, paste it into the Exchange Management Shell at the command prompt, and then run it. This command will set the Outlook certificate to *.xxxCustomDomainxxx.xxx:

    Set-OutlookProvider EXPR -CertPrincipalName:*.xxxCustomDomainxxx.xxx

16. Close your Exchange Management Shell window.

17. Close Notepad (do not save the untitled document).

18. To enable Exchange for the custom domain, you must identify the Exchange services that you want to assign to the *.xxxCustomDomainxxx.xxx certificate.

    If you have a tab open in your Edge browser for the on-premises **Exchange admin center,** then proceed to the next step; otherwise, select the **Windows** icon on the taskbar, select the **Microsoft Exchange Server 2019** group, select **Exchange Administrative Center.**

Note: If you receive a page indicating **This site is not secure**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select **More information**, and then select **Go on to the webpage (not recommended)**.

19. In the **Exchange Admin Center**, log in as **adatum\Administrator** with a password of **Pa55w.rd**.
20. In the **Exchange admin center**, select **servers** in the left-hand navigation pane.
21. On the **servers** page, the **servers** tab is displayed by default in the list of tabs across the top of the page. Select the **certificates** tab.
22. In the list of certificates, select the **wildcard_xxxCustomDomainxxx_xxx** certificate (where xxxCustomDomainxxx_xxx is the name of your accepted domain) and then select the **pencil (Edit)** icon on the menu bar.
23. You will now specify the Exchange services that you want to assign to this certificate for your accepted domain. In the **wildcard_xxxCustomDomainxxx_xxx** window, select **services** in the left-hand pane.
24. In the list of services, select the **SMTP** check box and the **IIS** check box, and then select **Save**. Select **Yes** in the **Warning** dialog box that appears.
25. In the **Exchange admin center**, select **mail flow** in the left-hand navigation pane and then select the **accepted domains** tab at the top of the page.
26. In the list of accepted domains, you must set the **A.Datum** domain (where the **Accepted Domain** is xxxUPNxxx.xxxCustomDomainxxx.xxx) as the Default domain. Select this domain (if it's not already selected by default), then select the **pencil (Edit)** icon on the menu bar above the list of domains.
27. In the **A.Datum** window, under the **This accepted domain is** setting, verify the **Authoritative** option is selected (this should have been set to Authoritative in the step 6 PowerShell command). Then select the **Make this the default domain** check box and select **Save**.

    In the list of domains, the **A.Datum** domain should now be listed as the **default domain** and the **Domain Type** should be **Authoritative**.
28. Close the Edge browser so that you close the Exchange admin center and proceed to the next task.

26.5 Task 5: Migrate On-premises User Accounts to the Custom Domain

In this lab, you will log into the Domain Controller (LON-DC1) VM and enable directory synchronization. To do this, you must first download the setup wizard for the Microsoft Azure Active Directory Connect tool. You will then run the installation wizard to enable and configure directory synchronization. This will perform a full synchronization that migrates all of Adatum's on-premises user accounts to the new accepted domain in Microsoft 365.

1. Switch to **LON-DC1** and, if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your Edge browser session, the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab should still be open; if not, then navigate to them now.

   Select the **Microsoft 365 admin center** tab, which should be displaying the **Domains** page.
3. In the **Microsoft 365 admin center**, in the left-hand navigation pane, select **Users**, and then select **Active users**.
4. You are now going to navigate to the **Microsoft Download Center** to download the **Azure AD Connect** tool.

   In the **Active users** window, on the menu bar, select the **ellipsis (More actions)** icon, and then in the drop-down menu that appears, select **Directory synchronization**.

   Note: If the **ellipsis (...)** icon does not appear on the menu bar, then at the very top of the left-hand navigation pane, select the **Navigation menu (three vertical lines)** icon to minimize the navigation pane, which removes the text. This expands the size of the **Active users** page, so the ellipsis icon should now appear on the menu bar. If for some reason you cannot locate the **Directory synchronization** option, then you can navigate directly to the **Azure AD Connect** page in the **Microsoft Download Center** by opening a new tab in your Edge browser and entering the following URL in the address bar

(if you navigate directly to this URL, you can skip the next step): **https://www.microsoft.com/en-us/download/details.aspx?id=47594**

5. In the **Azure Active Directory preparation** window, select **Go to the Download center to get the Azure AD Connect tool**. This opens a new tab in your browser and takes you to the Microsoft Download Center.
6. In the **Microsoft Download Center**, scroll down to the **Microsoft Azure Active Directory Connect** section and select the **Download** button.
7. The notification bar at the bottom of the page will display the status of the download operation. Once the download is complete, select **Open file** that appears below the **AzureADConnect.msi** file.
8. This initiates the installation of the **Microsoft Azure Active Directory Connect Tool**.

   Note: After the wizard begins, the **Microsoft Azure AD Connect Tool** window may disappear. If this occurs, find the icon for it on the task bar and select it.

   On the **Welcome to Azure AD Connect** window in the setup wizard, select the **I agree to the license terms and privacy notice** check box and then select **Continue**.
9. On the **Express Settings** page, read the instruction regarding a single Windows Server AD forest (which is the scenario in your VM lab environment) and then select **Use express settings**.
10. On the **Connect to Azure AD** window, you must enter the user credentials for a Microsoft 365 user account that has been assigned the Microsoft 365 Global Administrator role. Enter **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) in the **USERNAME** field, enter (or copy and paste) the tenant email password provided by your lab hosting provider in the **PASSWORD** field, and then select **Next.**

    Note: You may have to tab out of the **PASSWORD** field to enable the **Next** button.
11. On the **Connect to AD DS** page, enter **adatum\Administrator** in the **USERNAME** field, enter **Pa55w.rd** in the **PASSWORD** field, and then select **Next.**

    Note: You may have to tab out of the **PASSWORD** field to enable the **Next** button.
12. In the **Azure AD sign-in configuration** window, select the **Continue without matching all UPN suffixes to verified domains** check box at the bottom of the page and then select **Next**.
13. On the **Ready to configure** screen, select the **Start the synchronization process when configuration completes** check box (if it's not already selected), and select the **Exchange hybrid deployment** check box since you are preparing Azure AD Connect for an Exchange hybrid deployment.

    Select **Install**.
14. The installation will usually take 5 to 10 minutes to complete. On the **Configuration complete** window, verify you receive a message at the top of the window indicating **Azure AD Connect configuration succeeded.** Ignore the warning indicating the Active Directory Recycle Bin is not enabled for your forest. This recycle bin will not be needed for the purposes of this VM lab environment.

    Select **Exit**.
15. In the taskbar at the bottom of the screen, select the **magnifying glass (Search)** icon, and then in the Search box, enter **sync**. In the menu that appears, select the **Synchronization Service** desktop application to open it.
16. Maximize the **Synchronization Service Manager** window.
17. In the **Synchronization Service Manager** window, on the ribbon at the top of the page, the **Operations** tab is displayed by default so that you can monitor the synchronization process.
18. Wait for the **Export** profile to complete for **xxxxxZZZZZZ.onmicrosoft.com** (the second task in the list); when it finishes, its **Status** should be **completed-export-errors**.

    Once this status appears, select this row.
19. In the bottom portion of the screen, a detail pane appears showing the detailed information for this operation that you just selected.

- In the **Export Statistics** section, note the number of users that were added and the number that were updated.
- In the **Export Errors** section on the right, note the two errors that appear. Select the link for the first error that appears under the **Export Errors** column.

  The first error is an "add user"" error for user **Ngoc Bich Tran**. Review the error and then close the window. Select the link for the second error, which is an "add user" error for user **An Dung Dao**. Review this error and then close the window.
- So why did synchronization fail for these two users?

  To find out, select the **DataValidationFailed** link for the first error (under the **2 Error(s)** column). In the window that appears, select the **Detail** button. The **Error Information** window that appears indicates Ngoc Bich Tran's on-premises user account has an invalid UPN, which in turn caused a UPN validation error during the synchronization process; therefore, Ngoc's on-premises user account was not synchronized to Microsoft 365 by the Azure AD Connect tool. Select **Close** to close this window, and then select **Close** to close the Error Information window.

  If you select the **DataValidationFailed** link for the second error and then select the **Detail** button, you will note that An Dung Dao experienced the same UPN validation error.
- **IMPORTANT:** Because a synchronization had not been performed prior to this, the initial synchronization was a **Full Synchronization** (see the **Profile Name** column in the **Connector Operations** pane at the top of the page). Because the synchronization process will continue to run automatically every 30 minutes, any subsequent synchronizations will display **Delta Synchronization** as its **Profile Name**.

  If you leave the **Synchronization Service Manager** window open, after 30 minutes you will see that it attempts to synchronize the two users who were not synchronized during the initial synchronization. This operation will display as a **Delta Synchronization**.

20. Close the **Synchronization Service Manager**.
21. In your Edge browser, close the **Download Microsoft Azure AD Connect** tab, and then in the **Microsoft 365 admin center** tab, close the **Azure Active Directory preparation** pane. This will return you to the **Active users** list.

    Note: If you had to select the **Navigation menu** icon at the very top of the left-hand navigation pane in the earlier step to see the ellipsis icon, then select this **Navigation menu** icon again to expand the pane and display the text associated with each icon. Seeing the text associated with each icon makes it easier to navigate through the admin center.
22. On the **Active users** page, note that all the existing Microsoft 365 user accounts are the predefined users that were created in your tenant by your lab hosting provider.

    Select **Refresh** on the menu bar to see all the on-premises user accounts that were migrated to the new accepted domain in Microsoft 365.

    Note the **Username** for each of these accounts, which should be in the format of **<alias>@xxxUPNxxx.xxxCusto**
    Also note that each of these user accounts is **Unlicensed**; this indicates that while the on-premises accounts have been migrated to the new domain in Microsoft 365, they have not been assigned an Office 365 license.

    If you scroll down through the list of **Active users**, note that you will see both unlicensed and licensed users; the licensed users are the original list of Microsoft 365 user accounts created by your lab hosting provider.
23. On the right-side of the menu bar at the top of the page, select **Filter**. In the menu that appears, select **Licensed users**. This will display only those user accounts that were all assigned an Office 365 license (these are the Microsoft 365 user accounts that were created by your lab hosting provider).

    In the **Username** column, note how these user accounts were assigned to the **xxxxxZZZZZZ.onmicrosoft.com** domain when they were created by your lab hosting provider.
24. Note how the **Filter** option on the menu bar now displays **Licensed users**. Select **Licensed users** and in the menu that appears, select **Unlicensed users**. This will display all the user accounts that were just mi-

grated from the on-premises **adatum.com** domain to the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain. The migration process did not assign a license to any of these new Microsoft 365 accounts that were just created. If you scroll down through this list, you should not see any of the licensed user accounts in the **xxxxxZZZZZZ.onmicrosoft.com** domain.

In the **Username** column, note how these user accounts were assigned to the **xxxUPNxxx.xxxCustomDomainxxx.x** domain that you earlier created in Microsoft 365.

25. The **Filter** option on the menu bar should now display **Unlicensed users**. Select **Unlicensed users** and in the menu that appears, select **All users**. This will return you to the list of all active user accounts in both the **xxxUPNxxx.xxxCustomDomainxxx.xxx** and **xxxxxZZZZZZ.onmicrosoft.com** domains.

    Congratulations! You have just verified that the Full Synchronization process migrated Adatum's on-premises user accounts to the new accepted domain.

26. Leave your Edge browser and all tabs open as it will be used in the next lab.

27 End of Lab 9

28 Module 12 - Lab 10 - Exercise 1 - Configure Your Hybrid Deployment

In this lab you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. Adatum has decided to transition from their current on-premises Exchange Server 2019 deployment to a hybrid deployment that also utilizes Microsoft 365 Exchange Online.

In the prior lab, you prepared Azure Active Directory to support the hybrid synchronization between Adatum's on-premises Exchange Server 2019 environment and their cloud-based Exchange Online deployment. In this lab, you will set up Exchange for a hybrid deployment. This will require that you:

- Run the Hybrid Configuration Wizard (HCW) to create your hybrid deployment
- Configure Exchange admin center (EAC) settings to accommodate cloud and on-premises users within the same domain
- Configure the Outbound Connector from Microsoft 365 to your Exchange Server

To set up Exchange for a hybrid deployment, you must first run the Hybrid Configuration Wizard on your Exchange Server (LON-EX1). Once your hybrid deployment is installed, you will then test your hybrid deployment in the next exercise to verify that it's functioning properly.

28.1 Task 1: Create Adatum's Hybrid Exchange deployment

In this task, you will download and install the Hybrid Configuration Wizard (HCW) on the Exchange Server (LON-EX1) using the Exchange admin center for Exchange Online. Running the HCW will create Adatum's hybrid deployment.

1. Switch to **LON-EX1** and, if necessary, log in as the **Administrator** account with a password of **Pa55w.rd**.
2. Select the Microsoft Edge icon on the taskbar to open a new browser session, then enter the following URL in the address bar: **https://portal.office.com**
3. In the **Sign in** window, enter your tenant admin username (admin@xxxxxZZZZZZ.onmicrosoft.com, where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) and select **Next**.

    In the **Enter password** window, enter the tenant admin password provided by your lab hosting provider and then select **Sign in**.

4. In the **Stay signed in?** window, select the **Don't show this again** check box and select **Yes**.
5. In the **Microsoft Office Home** page, in the column of Microsoft app icons on the left-side of the screen, select the **Admin** icon.

6. In the **Microsoft 365 admin center**, select **Show all** in the left-hand navigation pane and under **Admin centers**, select **Exchange**. This will open the EAC for Exchange Online.
7. In the **Exchange admin center** for Exchange Online, the **dashboard** tab in the left-hand navigation pane is displayed by default, which displays the **Welcome** page.

   Scroll to the bottom of the **Welcome** page and under the **hybrid** section, select **setup**.
8. On the **setup** page there are two **configure** buttons. The first button configures an Exchange hybrid deployment, while the second button downloads the Exchange Online PowerShell module for supporting Multi-factor authentication.

   Select the first **configure** button to configure Adatum's hybrid deployment.
9. A new tab will open in your Edge browser, and in the **Open this file?** window that appears at the top of the page, select **Open**.

   This will initiate the **Application Install** wizard, which will download and install the Hybrid Configuration Wizard.
10. If the wizard begins and a **Do you want to install this application?** window appears, then proceed to the next step.

    However, because of security features in the VMs within your lab hosting environment, this wizard may not appear. Instead, when you select the **configure** button, the system may open a new tab, try to access a site, then close the tab and return to the **setup** page with the two **configure** buttons. If this occurs, then you must perform the following steps to open an **InPrivate Browsing** session within Edge to bypass the security constraints built into your training lab environment (this would not occur in a real world scenario). You will then open the Microsoft 365 admin center and initiate the hybrid deployment process.

    - To open an InPrivate Browsing session, right-click the **Edge browser** icon on the taskbar and in the menu, select **Start InPrivate Browsing**. This will open a new, InPrivate Edge session that is separate from the Edge session that you were just in.
    - Maximize the InPrivate browser window (if necessary), repeat steps 2 through 9, and then continue with the next step to install the Hybrid Configuration Wizard.

11. In the **Application Install** wizard, on the **Do you want to install this application?** window, select **Install** to download the Hybrid Configuration Wizard.
12. After the download completes, on the **Hybrid Configuration Wizard** window, select **next** to run the wizard.

    This starts the **Hybrid Configuration Wizard** (it can sometimes take up to a minute or so for the setup wizard to start, so please be patient).
13. The wizard begins by trying to detect the on-premises Exchange Server. Wait for the server detection to complete, which then displays the **On-premises Exchange Server Organization** window. The **Detect the optimal Exchange server** option will be selected by default, and the wizard will detect the **LON-EX1** server.

    Accept the default settings by selecting **next**.
14. The next page displays the **On-premises Exchange Account** and the **Office 365 Exchange Online Account**.

    Under the **Office 365 Exchange Online Account** section, select the **sign in...** button.
15. In the **Sign in** window, enter the tenant email account provided by your lab hosting provider (**admin@xxxxxZZZZZZ.onmicrosoft.com**; in a real-world scenario, this must be a Microsoft 365 user who has been assigned the Global Admin role) and then select **Next**.

    In the **Enter password** window, enter the tenant email password provided by your lab hosting provider and then select **Sign in**.

16. This returns you to the **On-premises Exchange Account** page, which now displays the **Tenant Email** account that you entered for the **Office 365 Exchange Online Account**.

    Once the account appears (which may take a few seconds), select **next**.

17. On the **Gathering Configuration Information** page, wait until the information gathering process is complete for both **Exchange** (on-premises) and **Office 365** (Exchange Online). Once both indicate they have **Succeeded** (which may take a minute or two), select **next**.

18. On the **Hybrid Features** page, select the **Full Hybrid Configuration** option and then select **next**.

19. On the **Hybrid Topology** page, the **Use Exchange Classic Hybrid Topology** option is selected by default.

    Note: We want you to use this **Classic** option instead of the **Modern** option so that you gain experience creating the necessary connectors in this wizard. The Modern option uses an agent to create the connectors between Exchange on-premises and Exchange Online, whereas the Classic option still configures the connectors, but does not use an agent to do so. In addition, since we are using published endpoints through the Domain Controller, it's preferable to use the Classic option. If we used a third-party such as godaddy, then the Modern option would be preferable.

    Verify the **Use Exchange Classic Hybrid Topology** option is selected and then select **next**.

20. On the **On-premises Account for Migration** page, select the **enter...** button to enter the credentials to your on-premises Exchange Web Service.

21. In the **Office 365** window that appears, the **Domain\username** is already prefilled with the **ADATUM\Administrator** account. Enter **Pa55w.rd** in the **Password** field and then select **ok.**

22. On the **On-premises Account for Migration** page, the **ADATUM\Administrator** account is displayed, so select **next**.

23. On the **Hybrid Configuration** page, verify the **Configure my Client Access and Mailbox servers for secure mail transport (typical)** option is selected by default (select it if necessary) and then select **next**.

24. On the **Receive Connector Configuration** page, select the drop-down arrow. This displays the **LON-EX1** server. Select the check box for this server and then select **next**.

25. On the **Send Connector Configuration** page, select the drop-down arrow. This displays the **LON-EX1** server. Select the check box for this server and then select **next**.

26. On the **Transport Certificate** page, select the drop-down arrow. This displays several existing certificates. Select the ***.xxxCustomDomainxxx.xxx** certificate (where xxxCustomDomainxxx.xxx is the lab hosting provider's custom domain name) and then select **next.**

27. On the **Organization FQDN** page, enter **xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx is your unique UPN name assigned to your tenant by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's custom domain) and then select **next**.

28. On the **Ready for Update** page, select **update.**

29. This initiates the configuration process, which usually takes a few minutes to complete.

    - If the configuration is successful, you will receive a **Congratulations!** page that indicates hybrid services are now configured between Exchange Online in your Office 365 tenant and your on-premises Exchange environment. If you receive this window, then select **close.**
    - If the configuration fails, it's typically the result of an **Access is Denied** error. As you just saw, there are several pages in the setup wizard that require you to enter username and password credentials. The wizard does not validate the credentials at the time you enter them; rather, it simply stores them and then validates the credentials in this final configuration step. Experience has shown that an **Access is Denied** error is usually the result of entering an incorrect username and/or password (for example, if you copy and paste in a username or password, copying in a trailing space after the username or password will cause it to fail).

      IMPORTANT: If you receive an **Access is Denied** error (or any error), you can simply repeat this entire task and re-run the Hybrid Configuration Wizard, which has been designed to allow multiple

re-runs without negatively affecting the system.

30. If you had to open an InPrivate browsing session to run the HCW, then close the InPrivate session.
31. In your Edge browser, close all tabs except for the **Microsoft Office Home** tab, the **Microsoft 365 admin center** tab, and the **Exchange admin center** tab.

28.2 Task 2: Configure Mail Flow Settings

In this task, you will configure mail flow settings in both the on-premises Exchange admin center (EAC) and the EAC for Exchange Online. First, you will log into the Exchange Server (LON-EX1) VM and then, through the on-premises EAC, you will configure the onmicrosoft.com domain so that on-premises users can send emails to cloud users within the same domain.

Second, you must verify the default settings in the Microsoft 365 EAC so that emails from cloud users to on-premises users in the same domain do not get stuck in an internal loop and never make it to their recipients' on-premises mailboxes.

IMPORTANT: You will open BOTH Exchange admin centers in this task in your LON-EX1 VM. Once you finish this task, you will leave both EAC's open on LON-EX1 for future tasks in this exercise.

1. You should still be logged into LON-EX1; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. Select the **Windows** icon on the taskbar and in the menu that appears, select the **Microsoft Exchange Server 2019** group. In the expanded group, select **Exchange Administrative Center**.

   This will open a new tab in your current Edge browser session that will display the on-premises Exchange admin center.

   Note: If you receive a page indicating **Your connection isn't private**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select the **Advanced** button, and then select **Continue to localhost (unsafe)**.
3. In the on-premises **Exchange Admin Center**, log in as **adatum\Administrator** with a password of **Pa55w.rd**.
4. In the on-premises **Exchange admin center**, select **mail flow** in the left-hand navigation pane, and then select the **accepted domains** tab at the top of the page.
5. In the list of accepted domains, select the **xxxxxZZZZZZ.mail.onmicrosoft.com** domain (where xxxxxZZZZZZ is the tenant prefix provided by the lab hosting provider).
6. Note the **Domain Type** for this onmicrosoft.com domain is set to **Authoritative**. You must change it to **Internal relay**. To do so, select the **pencil (Edit)** icon on the menu bar above the list of domains.
7. In the **xxxxxZZZZZZ.mail.onmicrosoft.com** window that appears, under the **This accepted domain is:** setting, select the **Internal relay** option and then select **Save**.
8. On the **mail flow** page, select the **send connectors** tab that appears at the top of the page.
9. In the list of send connectors, select the **Outbound to Office 365** connector and then select the **pencil (Edit)** icon on the menu bar.
10. On the **Outbound to Office 365** send connector window that appears, select the **scoping** tab in the left-hand navigation pane.
11. Under the **Address space** group at the top of the page, select the **plus (+) sign** icon to add the accepted domain.
12. In the **add domain** window, in the **Full Qualified Domain Name (FQDN)** field, enter ***.xxxCustomDomainxxx.xxx** (where xxxCustomDomainxxx.xxx is the lab hosting provider's custom domain name) and then select **Save.**
13. In the **Outbound to Office 365** send connector page, select **Save**.
14. You are currently in the on-premises EAC. You should also have the EAC for Exchange Online open in your Edge browser from the prior task (see the **setup − Microsoft Exchange** tab); if so, select this tab.

    However, if you closed the EAC for Exchange Online at the end of the prior task, then open it again by

entering the following URL (this shortcut saves you from navigating to the Office 365 home page, then to the Microsoft 365 admin center, and then to the EAC): **https://outlook.office365.com/ecp**

15. In the **Exchange admin center** for Exchange Online, in the left-hand navigation pane, select **mail flow**.
16. By default, the **rules** tab is displayed at the top of the page. Select the **accepted domains** tab.
17. In the list of accepted domains, select the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain (this is the accepted domain that you added in the prior lab exercise) and then select the **pencil (Edit)** icon.
18. In the **xxxUPNxxx.xxxCustomDomainxxx.xxx** window, under the **This accepted domain is:** setting, select the **Internal relay** option, select **Save**, and then select **OK** once the information has been successfully saved.
19. On the **mail flow** page, select the **connectors** tab at the top of the page.

    Note: There are several differences between the on-premises EAC and the EAC for Exchange Online. In the on-premises EAC, the **connectors** tab is split out into a separate **receive connectors** tab and a separate **send connectors** tab. In the EAC for Exchange Online that you are currently viewing, only one **connectors** tab is available.
20. In the **connectors** tab, the list of connectors displays an **Inbound** and **Outbound** connector. You must validate the settings for the **Inbound** connector, which is already selected by default. Therefore, simply select the **pencil (Edit)** icon.
21. On the **Edit Connector** window that appears, the name and description of the Inbound connector is displayed. Select **Next**.
22. On the **Edit Connector** page that asks **How should Office 365 identify email from your email server**?, verify the option is selected that asks: **By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended).**

    You should also verify that ***.xxxCustomDomainxxx.xxx** is displayed in the corresponding domain name field below this **"By verifying..."** option (where xxxCustomDomainxxx.xxx is the lab hosting provider's custom domain name); if not, you should enter this ***.xxxCustomDomainxxx.xxx** now. Select **Next**.
23. On the **Confirm your settings** page, select **Save**, and then select **OK** once the information is successfully saved.
24. Leave the two Exchange admin center tabs open in your Edge browser session and proceed to the next task.

28.3 Task 3: Prepare for testing by creating on-premises user mailboxes

In this task, you will remain in your Exchange Server (LON-EX1) VM, navigate to the on-premises Exchange admin center, and then create on-premises mailboxes for Allan Yoo and Beth Burke. You will later use Allan and Beth to test your hybrid deployment.

1. You should still be logged into LON-EX1; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your **Edge browser**, you should have the two **Exchange admin center** (EAC) tabs open from the earlier tasks in this exercise – one for the on-premises EAC and one for the EAC for Exchange Online.
   - One EAC tab should be titled **send connectors – Microsoft Exchange.** This is the on-premises EAC. Select this tab and note that in the left-hand side of the blue bar at the top of the page, it displays **Enterprise** and **Office 365**. This will help you identify this as the on-premises EAC.
   - The second EAC tab should be titled **connectors – Microsoft Exchange**. This is the EAC for Exchange Online. Select this tab and note that it does not include the blue bar with the **Enterprise** and **Office 365** options. This will help you identify this as the EAC for Exchange Online.

     Select the **send connectors – Microsoft Exchange** tab to display the on-premises EAC.
3. In the on-premises **Exchange admin center**, select **recipients** in the left-hand navigation pane. The **mailboxes** tab at the top of the page is displayed by default.

Note: Even though there are numerous on-premises user accounts (as noted by the on-premises user accounts that you previously synchronized into Microsoft 365), only one of those users had an on-premises mailbox set up in Exchange Server 2019 by your lab hosting provider. This user was the **Administrator** account, which is the only on-premises mailbox in the list.

In the remaining steps in this task, you will add on-premises mailboxes for two additional on-premises user accounts.

4. In the **mailboxes** tab, select the **plus (+) sign** icon on the menu bar to add a new on-premises mailbox. In the drop-down menu, select **User mailbox**.
5. In the **new user mailbox** window, you want to create a mailbox for Allan Yoo, who's an existing on-premises user. You can leave the **Alias** field blank as this will default to the user's first name as long as there is no conflict with the alias for an existing mailbox.
6. The **Existing user** option is selected by default, so select the **Browse** button next to the existing user field.
7. In the **Select User** window, select **Allan Yoo** in the list of users and then select **OK**.
8. In the **new user mailbox** window, select **Save**. In the list of mailboxes, Allan Yoo's mailbox should now appear. You will use Allan's on-premises mailbox when testing the Outbound Connector that you create in the next task.
9. Repeat steps 4 through 8 to create an on-premises mailbox for **Beth Burke**. You will use Beth's on-premises mailbox when testing mailbox migration in the next lab exercise.

   Allan and Beth's mailboxes should now appear in the list of mailboxes along with the Administrator's mailbox.
10. Leave your browser and all its tabs open and proceed to the next task.

28.4 Task 4: Create a new Outbound Connector

In this task, you will remain in your on-premises Exchange Server (LON-EX1) VM. In the EAC for Exchange Online, you will delete the existing outbound connector from Microsoft 365 to Adatum's on-premises Exchange Server (LON-EX1), and you will create a new outbound connector to take its place.

The short version as to why you must do this is because the VM lab environment for this course has a limitation related to updating a Microsoft Exchange certificate from a third-party certificate authority (CA); therefore, you must perform this workaround to bypass this issue with your lab environment.

The long version as to why you must do this begins with the fact that, by default, the existing Outbound connector has a dependency domain registration. Yet because you recently changed domains, the self-signed certificate is pointing to the adatum.com domain on LON-EX1 (your Exchange Server), while the third-party wildcard certificate for the xxxCustomDomainxxx.xxx domain also points to LON-EX1. Since the xxxCustomDomainxxx.xxx is not registered to the Exchange server, routing by the domain name will not work.

So how does this affect the Outbound connector? Well, normally at this point in the hybrid configuration process, you would validate the existing Outbound connector by using the primary domain name to route message traffic. However, because one of the two domain names isn't a registered point for your Microsoft Exchange Server, the validation of the Outbound connector will fail because the third-party certificate domain for the xxxCustomDomainxxx.xxx domain has not been validated to this Exchange Server.

In a real-world scenario in which you replace or add the domain just to your domain controller, you would update your Microsoft Exchange server certificate to point to the new domain. Unfortunately, the VM lab environment has a dependency to using Adatum.com as the primary domain; therefore, changing the domain would cause several communication issues with all the existing domain PC's and servers.

As a result, you must perform this workaround in the VM lab environment in which you delete the existing Outbound connector and then create a new one that routes email messages to the IP address associated with the Microsoft 365 tenant provided by your lab hosting provider. This removes the dependency between the Outbound connector and the Microsoft Exchange certificate that points to the Adatum.com domain, which in turn bypasses the conflict in which two domains point to the same Exchange Server.

STOP: After finishing the previous task, you should wait at least 15 minutes before starting this task. The reason for this delay is that when you created the on-premises Exchange mailboxes for Allan Yoo and Beth

Burke, it can take up to 15 minutes to propagate those updates throughout the system. **If you do not wait at least 15 minutes before starting this task, there is a good chance it will fail.**

1. You should still be in LON-EX1 after having completed the prior task; if necessary, log into LON-EX1 as the **Administrator** with a password of **Pa55w.rd**.
2. In your **Edge browser**, you should still have the two EAC tabs open from the earlier task – one for the on-premises EAC and one for the EAC for Exchange Online.
3. In your browser, select the **connectors – Microsoft Exchange** tab in your browser. This tab displays the EAC for Exchange Online.
4. In the **Exchange admin center** for Exchange Online, in the left-hand navigation pane, select **mail flow**.
5. Select the **connectors** tab at the top of the page.
6. You will begin by deleting the existing Outbound connector. The list of connectors currently displays an Inbound and Outbound connector. Select the **Outbound** connector to highlight it.

   NOTE: The Details pane on the right-side of the screen displays the details of the Outbound connector. Under the **Mail flow scenario** section, it indicates that this is the outbound connector from Office 365 to your organization's (on-premises) email server (which in Adatum's deployment is LON-EX1).
7. With the **Outbound** connector highlighted, select the **trash can (Remove)** icon on the menu bar.
8. On the **Warning** dialog box, select **Yes** to confirm that you want to delete this outbound connector. This will delete the outbound connector, which will be removed from the list of connectors.
9. You must now add a new Outbound connector. On the menu bar, select the **plus (+) sign** icon to add a new connector.
10. On the **Select your mail flow scenario** page, select the drop-down arrow in the **From** field and select **Office 365**.

    Then select the drop-down arrow in the **To** field and select **Your organization's email server**. Select **Next**.
11. On the **New connector** page, enter **Outbound connector to LON-EX1** in the **Name** field and then select **Next**.
12. On the next **New connector** page that asks **When do you want to use this connector?,** select the **For email messages sent to all accepted domains in your organization** option and then select **Next**.
13. On the next **New connector** page that asks **How do you want to route email messages?,** select the **plus (+) sign** icon.
14. In the **add smart host** window that appears, enter the **IP address** provided by your lab hosting provider (for example, 64.64.221.224) for your Microsoft 365 domain and then select **Save**.

    Note: In a real-world environment, you would typically enter a Fully qualified domain name (FQDN) here. However, given the settings of the VM lab environment, we instead must enter the IP address of our email server to bypass an internal conflict that appears to exist between Microsoft 365, the new xxxUPNxxx.xxxCustomDomainxxx.xxx domain, and the adatum.com domain.
15. On the **New connector** page that asks **How do you want to route email messages?,** the IP address should be displayed in the smart host list. Select **Next**.
16. On the next **New Connector** page that asks **How should Office 365 connect to your email server**?, accept the default settings (if necessary, select them):
    - The **Always use Transport Layer Security (TLS) to secure the connection (recommended)** check box should be selected.
    - The **Issued by a trusted certificate authority (CA)** option should be selected.
    - Below the **Issued by a trusted certificate authority (CA)** option, select the **And the subject name or subject alternative name (SAN) matches this domain name** check box, and then enter ***. xxxCustomDomainxxx.xxx** (where xxxCustomDomainxxx.xxx is your accepted domain name) in the domain name field that appears below this check box, and then select **Next**.

17. On the **Confirm your settings** page, review the settings. If any settings need to be changed, select **Back** and then proceed back through the pages to fix whatever needs to be corrected. When all the settings are correct, select **Next**.

18. On the **Validate this connector** page, select the **plus (+) sign** icon to enter Allan Yoo's on-premises email address, which will be used to validate this connector.

19. On the **add email** window that appears, enter Allan Yoo's email address of **Allan@xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx is the unique UPN Name and xxxCustomDomainxxx.xxx is the custom domain name, both of which were provided by your lab hosting provider), select **OK**, and then select **OK** once the information is successfully saved.

    NOTE: If it's been less than 15 minutes since you completed the previous task in which you created the on-premises mailbox for Allan, then you may receive an error message indicating that the email address is invalid. If this occurs, select **Cancel**, then wait several more minutes and try again.

20. Allan's email address should now appear on the **Validate this connector** page. Select **Validate**.

21. Once the validation is complete, select **Close**. On the **Validation Result** page, the validation will either be successful, or it will have failed. Perform the appropriate steps below depending on which result you receive.

22. If the validation was successful, the two validation tasks should be displayed: **checking connectivity to the IP address** and **sending a test email to an on-premises user mailbox within this IP address**. The status of both tasks should be **Succeeded**.

    Select **Save**, and then select **OK** once the information is successfully saved. Proceed to the final step in this task; you can skip the remaining steps, which provide instruction on what to do if the validation failed. Since your validation was successful, you can skip to the final step.

23. If either of the validation tasks failed, select the failed task and then select the **pencil** icon to display the **Details** about that task. This will help you troubleshoot the issue that caused the task failure.

    - If the **Send test email** task failed with a message indicating it could not find the user's on-premises mailbox, it's usually because you did not wait at least 15 minutes after creating Allan Yoo's on-premises mailbox in the prior task before performing this task. If this occurs, wait several minutes, select the **Back** button, and then select the **Validate** button again.
    - However, if the **Send test email** task failed with a message indicating **The test email was routed out from O365 without using any connector**, our lab testing has indicated that is typically a false-positive error (due to the conflict mentioned earlier between our VM lab environment and Microsoft 365), and in fact, the test-email was successfully routed to Allan Yoo's on-premises mailbox.

      To verify this, select **Close** to close the detail window, and then on the **Validation Result** window, select **Save**. You should save the connector even though the validation failed. This will display a **Warning** dialog box confirming whether you want to save the connector even though the validation failed. Select **Yes**, and then select **OK** once the information is successfully saved.

24. To verify whether Allan received the validation email, select a new tab in your **Edge browser** and open **Outlook Web App** by entering the following URL: **https://xxxUPNxxx.xxxCustomDomainxxx.xxx/owa** (where xxxUPNxxx is the unique UPN name assigned to your tenant by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's custom domain).

    Note: If you receive a page indicating **Your connection isn't private**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select the **Advanced** button, and then select **Continue to localhost (unsafe)**.

25. In the **Outlook** sign in window, enter **adatum\Allan** in the **Domain\username** field, enter **Pa55w.rd** in the **Password** field, and then select **sign in**. If necessary, select your Language and Time Zone and select **Save**.

26. In Allan's Inbox, you may or may not see an email from **O365ConnectorValidation@xxxUPNxxx.xxxCustomDomainxxx.xxx**.

    - If you see this email, then open it. The message in the email indicates it was sent from Office 365 to check that an email could be delivered using the new connector.

Note: If the outbound connector validation indicated the test email failed to be delivered, the presence of this email indicates that it was, in fact, delivered to Allan's mailbox. In the next lab exercise, you will perform a task to further show the connectors are working in Adatum's hybrid deployment.

- If you do not see the test email, then typically what happened is that the Outbound connector did not finish its internal configuration by the time the validation process sent the email. When this occurs, the mail gets stuck in an internal loop and when the Hop count is eventually exceeded, the validation fails and the message is not delivered.

  In the event the test email did not appear in Allan's Inbox, you will revalidate the Outbound connector that you just created and saved. On the **connectors** page, you should see the Outbound connector that you created. Select the **Outbound connector to LON-EX1** and then select the **pencil (edit)** icon on the menu bar. This will walk you through all the steps that you previously performed to create and validate the connector (steps 12-21). However, this time, all the information that you entered when you created the connector will be prefilled for you, so you basically just have to select **Next** to proceed through each page.

  Chances are, if the validation failed the first time, it will fail again. However, this time, once it fails, select **Allan's mailbox tab** in your browser and you should see the validation email in his Inbox. By the time you run this validation a second time, the Outbound connector should have finished its configuration, so the mail should be delivered (even though from a validation standpoint, it does not think it did).

27. Leave your browser and all its tabs open and proceed to the next exercise.

29 Proceed to Lab 10 - Exercise 2

30 Module 12 - Lab 10 - Exercise 2 - Test your Hybrid Deployment

In the prior exercise, you configured Adatum's Exchange environment for a hybrid deployment. In this exercise, you will test your new hybrid deployment. This will require that you:

- Test the hybrid configuration by sending emails between on-premises and cloud users in Task 1
- Migrate a user mailbox from Exchange on-premises to Exchange Online to test your connectors in Task 2
- Test the newly migrated mailbox in Task 3

IMPORTANT: Migrating an on-premises mailbox to Microsoft 365 in Task 2 can take up to an hour to complete. Instead of waiting around for an hour before you can do Task 3, proceed to the Final Assessment lab once you start the migration at the end of Task 2. By the time you finish the Final Assessment lab, the migration process in Task 2 should hopefully be complete, at which time you can return to this lab and perform Task 3 to test the newly migrated mailbox.

30.1 Task 1: Test the Hybrid topology

In this task, you will verify that your hybrid environment is functioning properly by performing the following validation steps that send emails between an on-premises Exchange mailbox and a Microsoft 365 cloud mailbox:

- From your on-premises Exchange Server (LON-EX1) VM, you will first send an email from Allan Yoo's on-premises Exchange Server mailbox to Alex Wilber's cloud mailbox in Microsoft 365.
- You will then open an InPrivate Browsing session in Edge browser so that you can log into Alex's mailbox in Microsoft 365 and verify that he received the email from Allan.
- You will then send a reply from Alex's cloud mailbox to Allan's on-premises mailbox, and then verify that Allan received the reply.

Important: In this task, note what happens when you send the email from Allan's on-premises mailbox to Alex's Microsoft 365 mailbox; or more specifically, note where the email is delivered. This situation provides the basis for the Final Assessment lab.

1. You should still be logged into LON-EX1 from the prior exercise; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.

2. You are now going to send an email from Allan Yoo's on-premises mailbox to Alex Wilber's Microsoft 365 mailbox; therefore, you must sign into Outlook using Allan's on-premises email account.

   At the end of the prior lab exercise, if your Outbound connector validation failed and you verified that it was a false-positive error by opening Allan Yoo's on-premises mailbox to see the test validation email in his Outlook Inbox, then skip to step 5.

   However, if your Outbound connector validation succeeded in the prior lab exercise, then perform steps 3-4 to open Allan's on-premises mailbox.

3. If your Outbound connector validation succeeded in the prior lab exercise, then select a new tab in your **Edge browser** and open **Outlook Web App** by entering the following URL in the address bar: **https://xxxUPNxxx.xxxCustomDomainxxx.xxx/owa** (where xxxUPNxxx is the unique UPN name assigned to your tenant by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's custom domain).

   Note: If you receive a page indicating **Your connection isn't private**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select the **Advanced** button, and then select **Continue to localhost (unsafe)**.

4. In **Outlook**, enter **adatum\Allan** in the **Domain\user name** field, enter **Pa55w.rd** in the **Password** field, and then select **sign in**. If requested, select your **Language** and **Time zone** and then select **Save**.

5. In Allan's **Inbox**, you should see the email he received from the prior lab exercise in which the system validated the Outbound connector that you created.

   You should now send an email from Allan's on-premises mailbox to Alex Wilber's Microsoft 365 mailbox. Select **New** in the ribbon, and in the email's **To** address line, enter **alexw@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider).

6. Enter **Hybrid test - On-premises to M365 email** in the **Subject** line, enter **From Allan's on-premises mailbox to Alex's M365 mailbox** in the body of the email, and then select **Send**.

7. At this point, you want to log into Alex Wilber's Outlook mailbox in Microsoft 365 to verify he received the email from Allan Yoo's on-premises mailbox. You then want to send a reply from Alex's Microsoft 365 mailbox back to Allan's on-premises mailbox.

   IMPORTANT: Since you already have Allan's mailbox open in Edge browser, you CANNOT open Alex's mailbox in another tab in the same Edge session. Doing so will block email from Allan's on-premises account from being sent to Alex's Microsoft 365 account. **Therefore, you must start an InPrivate Browsing session and then open Alex's mailbox in that session.**

   To open an InPrivate Browsing session, right select the **Edge browser** icon on the taskbar and in the menu, select **New InPrivate window**. This will open a new, InPrivate Edge session that is separate from the Edge session that contains the tab with Allan's mailbox.

   Maximize the InPrivate browser window and enter the following URL: **https://portal.office.com**

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

9. In the **Enter password** window, enter your tenant email password provided by your lab hosting provider and then select **Sign in**.

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

11. In Alex's **Office 365 Home** page, note all the applications that are displayed in the column of Microsoft 365 apps on the left-siode of the screen. These are the apps that are enabled for Alex given his Office 365 E5 product license. Select the **Outlook** icon.

12. Alex's Microsoft 365 mailbox will open in **Outlook**. If a **Welcome** window appears, select **X** in the upper-right corner to close it.

13. Note that Allan's email to Alex does not appear in Alex's Inbox. However, select Alex's **Junk Email** folder. If the email sent by Allan appears in Alex's **Junk Email folder**, then open the email and reply to the message. Indicate in the reply that this message is from Alex's Microsoft 365 mailbox to Allan's

on-premises mailbox.

Important: There is a specific reason why Allan's email ended up in Alex's Junk Email folder rather than his Inbox. However, the reason will not be explained here, since this is the very issue covered in the next lab exercise, which is the Final Assessment lab. Once you complete the Final Assessment lab, you will understand why this occurred. For now, simply leave Allan's email in Alex's Junk Email folder and send your reply back to Allan as directed earlier in this step.

14. After sending Alex's reply back to Allan, hover over the **Edge browser** icon on the taskbar and select the session that displays **Allan's** on-premises mailbox. Verify that Allan received the reply from Alex (you may need to refresh the Inbox if the reply is not there when you return to Allan's mailbox).

    You have just verified that your hybrid environment is functioning properly.

15. Close the InPrivate Browsing session but leave your Edge browser session open.

16. There is another test that you can perform to validate that your connector worked properly, even though the validation may have failed. This test is a message trace.

    Select the **connectors – Microsoft Exchange** tab in your Edge browser to display the EAC for Exchange Online.

17. If you recall from an earlier lab in this course, the Message Trace functionality has been moved from the classic EAC to the **New Exchange admin center**. Therefore, in the (classic) **Exchange admin center**, in the left-hand navigation pane, select **New Exchange admin center.**

18. In the (New) **Exchange admin center**, select **Mail flow** in the left-hand navigation pane, and then in the expanded group, select **Message trace**.

19. On the **Message trace** window, the **Default queries** tab at the top of the page is displayed by default. In the list of queries and reports in this tab, select **Messages sent from my primary domain in the last day.**

20. In the **New message trace** pane that appears, the default values for the **Messages sent from my primary domain in the last day** query are displayed. You can control which messages are selected based on who sent and received the messages and how many days ago the messages were sent.

    All the default settings on this page are sufficient for this message trace that you want to perform, so none of the settings need to be changed:

    - **Senders.** You want to view email from all senders from the xxxUPNxxx.xxxCustomDomainxxx.xxx domain.
    - **Recipients.** You want to view email sent to all recipients.
    - **Time range.** You want to view all email sent in the past day.
    - **Report type.** You want to view the Summary report, which provides instant online access to the message trace search results.

    Since none of the settings need to be changed, simply select the **Search** button at the bottom of the page to initiate the message trace.

21. On the **Message trace search results** window, you should see each of the emails that have been sent and received:

    - the O365ConnectorValidation email from the Outbound connector validation process to Allan Yoo
    - the email you sent from Allan Yoo to Alex Wilber that was received into Alex's Junk Email folder (note the **Status** of this email, which is **FilteredAsSpam**)
    - the reply that you sent from Alex Wilber back to Allan Yoo

22. Close this **Exchange admin center** tab (for the New Exchange admin center) in your Edge browser.

23. In the Edge browser session, close the tab displaying Allan Yoo's Outlook mailbox. Leave the two EAC tabs open (for the classic EAC and the on-premises EAC) and proceed to the next task.

30.2 Task 2: Migrate an on-premises mailbox to test your connectors

In this task, you will log into your Exchange Server (EX1) VM, open the on-premises Exchange admin center, and migrate Allan Yoo's on-premises mailbox (along with his mail) to Microsoft 365. The purpose of this task is to verify whether your connectors are correctly set up and to provide a level of simplicity for the user.

When users are cloud-hosted they do not have to use a VPN tunnel to access company files; they can log in from any PC or device and work from any location that has a stable internet connection. In contrast, hosting mailboxes on-premises and accessing files typically requires a VPN tunnel to keep company data secure.

1. You should still be logged into LON-EX1 from the prior exercise; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your **Edge browser**, you should have the two **Exchange admin center** (EAC) tabs open from the prior exercise – one for the on-premises EAC and one for the EAC for Exchange Online.

   Select the **send connectors – Microsoft Exchange** tab to display the on-premises EAC.
3. In the on-premises **Exchange admin center**, in the left-hand navigation pane, select **recipients**, which displays the **mailboxes** tab by default. In the list of mailboxes, select **Allan Yoo**.
4. In the **Allan Yoo** details pane on the right, scroll down to the bottom, and under the **Move Mailbox** section, select **To Exchange Online**.

   Important: Prior to installing your hybrid Exchange deployment, if you looked at this **Move Mailbox** section for any of the on-premises mailboxes, you would not see the **To Exchange Online** option. However, once you install the hybrid deployment, the **To Exchange Online** option should appear for any of the on-premises mailboxes. If you do not see **To Exchange Online** under the **Move Mailbox** section, then the browser needs to be refreshed; in other words, you must close the tabs on your browser, then close the browser itself, and then re-open it. If you must do this, then start the on-premises **Exchange admin center**, log in as **adatum\Administrator** with a password of **Pa55w.rd**, navigate to **recipients** and the **mailboxes** tab, and then select **Allan Yoo's** mailbox. This time you should see the **To Exchange Online** option, which you should select.
5. In the **information** pop-up screen, select **sign in to Office 365**.
6. If the **new migration batch** window appears, then proceed to the next step; otherwise, if a **critical error** dialog window appears, then perform the following steps:
   - In the dialog window displaying the critical error message, select **OK.**
   - In the EAC, select **hybrid** on the left-hand navigation pane and then on the **setup** page, select the **modify** button. If an information pop-up window appears, select **sign in to Office 365**, and then sign in if required (if the sign in used your MOD Administrator credentials, then a sign in window will not appear).
   - In the blue heading line above **Exchange admin center** at the top of the window, it displays **Enterprise** and **Office 365**. Note the arrow is pointing to which EAC currently being displayed. Ensure that **Enterprise** (on-premises) is selected before you continue to the next step.

     If it is not selected at the top, close your browser and start again at step 1 of this task. However, if **Enterprise** is selected, then repeat steps 3 and 4, and then continue with the next step.
7. In the **new migration batch** window, if a sign in page appears (if it does not appear, then skip to the next step), enter **adatum\Administrator** in the **Account with privileges (domain\user name)** field, enter **Pa55w.rd** in the **Password of account with privileges** field, and then select **Next**.
8. On the **Confirm the migration endpoint** page, the **Remote MRS proxy server** should be set to **xxxUPNxxx.xxxCustomDomainxxx.xxx** by default, so simply select **Next.**
9. On the **Move configuration** page, enter **Migrating Allan Yoo** in the **New migration batch name** field, verify that **xxxxxZZZZZZ.mail.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by the lab hosting provider) is entered in the **Target delivery domain** field, and then select **Next**.
10. On the **Start the batch** page, under the **Please select the preferred option to complete the batch** section at the bottom of the page, select the **Automatically complete the migration batch** option and then select **new.**

11. On the **Information** pop-up windows that indicates **Saving completed successfully**, select **OK**.
12. On the **information** pop-up window that asks **Do you want to go to the migration dashboard to see the status of your migration batch?** select **Yes**.
13. On the **migration** page, monitor the status of the migration. The **Status** column will begin by displaying **Syncing,** and eventually it will change to **Completed**.

    IMPORTANT: Migrating an on-premises mailbox to Microsoft 365 can take up to an hour to complete. Therefore, once you have finished this task, proceed to the Final Assessment lab. Once you have finished the final assessment, return to this lab exercise and perform Task 3 to test the newly migrated mailbox.

30.3 Task 3: Test the newly migrated mailbox

The prior exercise migrated Allan Yoo's on-premises mailbox to Microsoft 365. In this task, you will validate whether Outlook features are working properly for Allan's new Microsoft 365 mailbox. When testing in a real-world environment, ensure that mail flow isn't impeded, and that the user can access his or her mail by going to **outlook.office365.com**. This ensures that no complications occurred during the migration process. As a best practice, you should always test your mail flow to validate a migration.

In this task, you will test mail flow by sending an email from Allan's new Microsoft 365 mailbox to Beth Burke's on-premises mailbox (which you created in the prior lab exercise). You will also send meeting requests from Allan to Beth. This task will verify whether your connectors are correctly set up.

1. You should still be logged into LON-EX1 after having completed the Final Assessment lab; if necessary, log in as the **Administrator** account with a password of **Pa55w.rd**.
2. On the **migration** page, monitor the status of the migration. The **Status** column will begin by displaying **Syncing,** and eventually it will change to **Completed**.

   NOTE: If you closed the migration tab and now want to return to it to check on the status of your migration, return to the EAC for Exchange Online, select **recipients** on the left-hand navigation bar, and then select **migration** on the ribbon. This will return you to the list of migration batches.

   IMPORTANT: You cannot perform this task until the mailbox migration is complete. If the migration did not complete while you were working on the Final Assessment lab, then you must wait until it finishes before proceeding.

   Note: You can select your migration batch and then select **View details** in the Details pane on the right side of the screen to see more information on the migration. The Details pane that appears also displays the batch status. HOWEVER, please note that this status is NOT the same as the status that displays on the **migration** window in the EAC for Exchange Online. The Details pane status is reflective of the objects being moved from on-premises to the cloud, so while this status may display **Completed**, that does NOT mean the migration is complete. In fact, this Details pane may indicate **Completed,** but the status on the migration window can still show **Syncing**. The reason for this is that even after the objects are moved, there are still several additional tasks that the migration must perform before it's complete.

   Important: In summary, you should NOT proceed to the next task until the status on the **migration** window displays **Completed** for your batch.

3. Since you just completed the Final Assessment lab prior to returning to this task, you should have Beth Burke's on-premises mailbox open in your Edge browser session, and you should have Alex Wilber's Microsoft 365 mailbox open in an InPrivate Browsing session. Therefore, you must close Alex's mailbox and open Allan's mailbox in the InPrivate Browsing session.

   You should begin by logging out of Microsoft 365 as Alex Wilber. Hover your mouse over the Edge browser icon on the taskbar, select Alex's mailbox tab in the InPrivate Browsing session. On Alex's mailbox, select Alex's user icon in the upper right corner of the screen and select **Sign out**.

   Once you are signed out as Alex, close the Microsoft Office Home tab in your InPrivate Browsing session.
4. On the **Sign out** tab in the InPrivate Browsing session, browse to **https://outlook.office365.com.** On the **Pick an account** window, select **Use another account.** On the **Sign in** window, enter

Allan@xxxUPNxxx.xxxCustomDomainxxx.xxx (where xxxUPNxxx is your unique UPN Name and xxxCustomDomainxxx.xxx is the accepted domain) and then select **Next**. On the **Enter password** window, enter **Pa55w.rd** and then select **Sign in**.

5. If prompted, select your **Language** and **Time zone** and then select **Save**.
6. If a **Welcome** window appears, then close it.
7. You are now signed into Allan's mailbox that was just migrated from the on-premises LON-EX1 Exchange Server to Microsoft 365. Note the emails in Allan's Inbox; these were messages he received when the mailbox was still on-premises. This verifies that his messages were migrated to Microsoft 365 along with his mailbox.

   Create a new test email and send it to **Beth Burke**. Beth's email address is **Beth@xxxUPNxxx.xxxCustomDomainxxx.xxx** (where xxxUPNxxx is your unique UPN Name and xxxCustomDomainxxx.xxx is the accepted domain).
8. At this point, you must log into Beth Burke's on-premises mailbox to verify she received the email from Allan Yoo's Office 365 mailbox. You then want to send a reply from Beth's on-premises mailbox back to Allan's Office 365 mailbox.

   Note: In the Final Assessment lab that you just completed, you opened Beth's on-premises mailbox to test your final assessment lab solution. Hover your mouse over the Edge browser icon on the taskbar and select Beth's mailbox.

   However, if you closed Beth's mailbox after the Final Assessment lab, then open it again in your Edge browser session (not in the InPrivate Browsing session that has Allan's mailbox open) by navigating to **https://xxxUPNxxx.xxxCustomDomainxxx.xxx/owa** and signing in as **adatum\beth** with a Password of **Pa55w.rd.**
9. The email that Allan just sent to Beth should appear in her **Inbox**. Open the email and reply to the message.
10. Hover over the **Edge browser** icon on the taskbar and select the InPrivate Browsing session that displays **Allan's** Microsoft 365 mailbox. If Beth's reply does not appear in Allan's **Inbox**, then refresh the Inbox.

    Seeing Beth's reply verifies that mail flow is working properly between an on-premises mailbox and Allan's newly migrated Microsoft 365 mailbox.
11. You will now test whether Calendar functionality is working properly in Allan's new Microsoft 365 mailbox. In Allan's mailbox, select the **calendar** icon in the bottom-left corner of the window.
12. Create a new meeting with a subject **Test meeting**.
13. Add **Beth Burke** as a required meeting attendee, then select **Scheduling Assistant**.
14. Both Allan and Beth's calendars will be displayed, and they should both show that their respective user is free. Select **Done** to accept the time and then select **Send** to send the meeting request to Beth.
15. Hover over the **Edge browser** icon on the taskbar and select **Beth's** on-premises mailbox.
16. In Beth's Inbox, **Accept** the meeting request and select **Send the response now**.
17. Hover over the **Edge browser** icon on the taskbar and select the InPrivate Session that's displaying **Allan's** calendar. Select the **email** icon in the bottom left-corner of the window and verify that Allan received the accepted meeting request from Beth.
18. Create another meeting request with a subject of **Test 2**. Add **Beth Burke** as a meeting attendee again, then select **Scheduling Assistant**.

    Beth's calendar should show her as busy for the first meeting request. Select **Discard** to close the Scheduling Assistant, select **Discard** to cancel the meeting request, and then select **OK** to confirm the cancelation.

    You have now verified that the mail flow is functioning properly between a newly migrated Microsoft 365 mailbox (Allan) and an on-premises mailbox (Beth). From within Allan's calendar, you can also access Beth's calendar to see her status when creating a meeting request. This verifies that your connectors are

correctly set up.

CONGRATULATIONS! You have completed all the labs in this course!

31 Module 12 - Lab 10 - Exercise 3 – Final Assessment

In this exercise, you will continue in your role as Holly Dickson, Adatum's Messaging Administrator. You have been tasked with resolving a messaging issue in Adatum's newly configured hybrid deployment.

You should use all the skills you have learned during this course to identify the issue and mitigate the following problem that Adatum is currently experiencing:

Problem: In your role as Adatum's Messaging Administrator, you have completed Adatum's hybrid Exchange deployment. However, several Adatum users have just informed you that emails are being delivered to their Junk Email folder rather than their Inbox. In fact, your CTO (Alex Wilber) is one of those users; he just stopped by your office to let you know that he did not receive an expected email from Allan Yoo, only to find out later that the email had been delivered to his Junk Email folder. This has added additional urgency to the problem.

The CTO wants you to figure out why emails are not being delivered properly. Use the tools in your environment to solve the issue.

Hint: Review the information in this course relating to message delivery. Compare that to what you did in the previous labs when you configured Adatum's hybrid deployment to determine what needs to be fixed to solve this problem. Once you think you have solved the problem, send an email from Beth Burke's on-premises mailbox to Alex Wilber's Microsoft 365 mailbox to see whether the email is treated as spam and delivered into Alex's Junk Email folder, or if it gets delivered into his Inbox.

Solution Guide: If you find yourself struggling with this problem and unable to determine how to resolve it, you can download the step-by-step solution guide for this Final Assessment lab. **However, in the spirit of learning, please try to resolve the issue on your own using the knowledge you have acquired in this course before turning to the solution guide.**

Reminder: Once you have finished with this lab, you should return to the previous lab exercise and complete Task 3, which tests whether the mailbox migration of Allan Yoo's on-premises mailbox to Microsoft 365 was successful.