Contents

1 MS-500X: Microsoft 365 Security Administrator

This repository includes lab instructions for the following courses:

- MS-500T00: Microsoft 365 Security Administration

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 and Microsoft 365 services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the 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 or Microsoft 365 services, and get the latest files for their delivery.

1.3 What about changes to the student handbook?

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

1.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new 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-500-Microsoft-365-Security/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MS-500-Microsoft-365-Security/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

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

In the following lab exercises you will take on the role of Holly Dickson, Adatum Corporation's Security Administrator. Adatum runs their legacy applications (such as Microsoft Exchange) in an on-premises deployment. However, they recently subscribed to Microsoft 365, thereby creating a hybrid deployment in which they must synchronize their on-premises and cloud deployments.

You have been tasked with deploying Microsoft 365 in Adatum's hybrid deployment using a virtualized lab environment. In this lab, you will set up a Microsoft 365 trial tenant, add a custom on-premises accepted domain, install Azure Active Directory, and add several users and groups that will be used throughout the remainder to the labs in this course.

In this lab, the trial tenant has already been selected and a default tenant admin account has already been created. In your role as Holly Dickson, Adatum's Security Administrator, you will be responsible for the remainder of the initial setup. You will log into the Domain Controller VM using the ADATUM\Administrator account, and when you access Microsoft 365 for the first time, you will initially log in using the tenant email account that has been assigned to your Microsoft 365 tenant. Once you create your Microsoft 365 account for Holly, you will log into Microsoft 365 as Holly from that point forward.

3.0.1 Task 1 - Obtain Your Office 365 Credentials

Once you launch the lab, a free trial tenant will be made available to you to access Azure in the Microsoft Virtual Lab environment. This tenant will be automatically assigned a unique username and password. You must retrieve this username and password so that you can sign into Azure and Microsoft 365 within the Microsoft Virtual Lab environment. You will also be assigned a unique network IP address and UPN name for your O365 blob. You will also use this UPN name in various tasks throughout the labs for this course.

1. Because this course can be offered by learning partners using any one of several authorized lab hosting providers, the actual steps involved to retrieve the UPN name, network IP address, and tenant ID associated with your tenant may vary by lab hosting provider. Therefore, your instructor will provide you with the necessary instructions on how to retrieve this information for your course. The information that you should note for later use includes:
   - **Tenant suffix ID.** This ID is for the onmicrosoft.com accounts that you will use to sign into Microsoft 365 throughout the labs. This is in the format of **{username}@M365xZZZZZZ.onmicrosoft.com**, where ZZZZZZ is your unique tenant suffix ID provided by your lab hosting provider. Record this ZZZZZZ value for later use. When any of the lab steps direct you to sign into the Office 365 or Microsoft 365 portals, you must enter the ZZZZZZ value that you obtained here.
   - **Tenant password.** This is the password for the admin account provided by your lab hosting provider.
   - **UPN name (in the format XXYYZZa) and the network IP address.** Write down the **IP Address** value (this is the IP Address of your parent domain; for example, 64.64.206.13), as well as your **UPN name** (for example, AVEAH2a).

3.0.2 Task 2- Set up the Organization Profile

In your role as Holly Dickson, Adatum's Security Administrator, you have been tasked with setting up the company's profile for its Microsoft 365 trial tenant. In this task, you will configure the required options for Adatum's tenant. Since Holly has yet to create a personal Microsoft 365 user account (you will do this in Task 3), Holly will initially sign into Microsoft 365 as the default Microsoft 365 MOD Administrator account using the Tenant email address and password that was assigned by your lab hosting provider.

1. When the Virtual Machine opens, it opens with the Client PC VM (**LON-CL1**). You need to switch to the Domain Controller VM (**LON-DC1**).
2. Log on as **ADATUM\Administrator** with the password `Pa55w.rd`.
3. If you receive a **Networks** warning message asking if you want this PC to be discoverable by other PCs and devices on this network, select **No.**
4. **Server Manager** will automatically start. Leave it open (it's used in the next task) but minimize the window for now.
5. On the taskbar at the bottom of the page, select the **Internet Explorer** icon. Maximize your browser window when it opens.
6. In your browser go to the **Microsoft Office Home** page by entering the following URL in the address bar: `https://portal.office.com/`
7. In the **Sign in** dialog box, copy and paste in the **Tenant Email** account provided by your lab hosting provider and then select **Next**.
8. In the **Enter password** dialog box, copy and paste in the **Tenant Password** provided by your lab hosting provider and then select **Sign in**.
9. On the **Stay signed in?** dialog box, select the **Don't show this again** checkbox and then select **Yes.**
10. If a **Get your work done with Office 365** type window appears, then close it now.
11. If a **Set your time zone** window appears, select **set the time zone for your calendar**. In the **Outlook** window that opens, under **Time zone,** select your time zone and select **Save**, then close your browser window and re-open the **Microsoft Office Home** page by entering the following URL in the address bar: `https://portal.office.com/`.
12. If a **Good morning/afternoon/evening MOD Administrator** window appears, select **Get started**.
13. In the **Microsoft Office Home** page, select the **Admin** app. This opens the **Microsoft 365 admin center.**
14. In the left navigation pane, select the **Show All** ellipsis … icon to display all the navigation menu options.
15. In the left navigation pane, select **Settings** and then select **Org Settings** then select **Organization profile** tab.
16. In the **Organization Profile** tab select **Organizational information**, it displays Contoso as the organization name, change this information.

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

17. In the **Organization information** window, enter the following information:

    - Name: `Adatum Corporation`
    - Address: `555 Main Street`
    - City: `Redmond`
    - State: **Washington**
    - Postal Code: `98052`
    - Phone: `425-555-1234`
    - Technical contact: **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
    - Preferred language: **select your preferred language**

18. Select **Save**.

19. Close the **Organization information** window.

20. In the Settings window select **Release preferences**.

21. In the **Release preferences** window, select **Targeted release for selected users** and then select **Save**.

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

22. If the **Are you sure you want to change to Targeted release for select people** window appears, select **Yes.**.

    Note: This option enables you to create a control group of users who will preview updates so that you can prepare the updates for your entire organization. The **Targeted release for everyone** option is more commonly used in development environments, where you can get updates early for your entire organization. In non-development environments, such as Adatum, targeted release to select people is the more typical preference as it enables an organization to control when it wants to make updates available to everyone once they've been reviewed by the control group.

23. In the **Release preferences** window, select **Select users**.

24. In the **Choose users for targeted release** window, in the list of users, select the **MOD Administrator** and then select **Save**.

25. Close the **Release preferences** window, this returns you to the **Settings** window.

26. Select **Custom themes**.

27. In the **Customize themes** window, you can add the logo of your company and set the background image as the default for all your users. Along with these options you can change the colors for your navigation pane, text color, icon color, and accent color. Go ahead and explore some different options for your tenant. Make any changes that you wish.

    Note: Some colors patterns aesthetically distract users. Avoid using high contrasting colors together, such as neon colors and high-resolution colors like white and bright pink.

28. Once you're done exploring and making any further changes, select **Save** and then **Close**.

29. Remain logged into the domain controller VM and in Internet Explorer, leave your Microsoft 365 admin center tab and all tabs open for the remaining tasks.

3.0.3 Task 3 - Create Microsoft 365 User Accounts

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

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

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

1. On the **LON-DC1** VM, the **Microsoft 365 admin center** should still be open in Internet Explorer from the prior task. In the **Microsoft 365 admin center**, in the left navigation pane, select **Users** and then select **Active users**.
2. In the **Active users** list, you will see the the default **MOD Administrator** account as well as some other user accounts. Since you're taking on the role of Holly Dickson in this lab scenario, you will create a user account for yourself, and you will assign yourself the Microsoft 365 role of Global Administrator.
3. In the **Active Users** window, select **Add a user**.
4. In the **Set up the basics** window, enter the following information:
    - First name: `Holly`
    - Last name: `Dickson`
    - Display name: When you tab into this field, **Holly Dickson** will appear.
    - Username: When you tab into this field, **Holly** may appear; if not enter this as the username

      IMPORTANT: To the right of the **Username** field is the domain field. It may be prefilled with the custom **XXYYZZa.CustomDomain.us** on-premises domain; however, you must select the drop-down arrow and select the **M365xZZZZZZ.onmicrosoft.com** cloud domain instead (where ZZZZZZ is your tenant ID provided by your lab hosting provider).

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

      Holly@M365xZZZZZZ.onmicrosoft.com
    - Password settings: Uncheck the **Automatically create a password** option
    - Password: `Pa55w.rd`
    - Uncheck the **Require this user to change their password when they first sign in** checkbox.
5. Select **Next**.
6. In the **Assign product licenses** window, enter the following information:
    - Select location: **United States**
    - Licenses: Under **Assign user a product license**, select **Office 365 E5** and **Enterprise Mobility + Security E5**.
7. Select **Next**.
8. In the **Optional settings** window, in the Roles section select **Admin center access** By doing so, all the Microsoft 365 administrator roles are now enabled and available to be assigned.
9. Select **Global Administrator** and then select **Next**.
10. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.
11. On the **Holly Dickson has been added to active users** page, select **Close.**

12. Remain logged into the domain controller VM with the Microsoft 365 admin center open in your browser for the next task.

3.0.4 Task 4 – Prepare for Microsoft Azure Active Directory

Azure Active Directory is needed to perform several configuration steps when installing Microsoft 365. These steps are performed using Windows PowerShell. However, before you can use PowerShell to access Azure AD, you must first install the Windows PowerShell modules that enable you to access Azure AD through PowerShell. In this task, you will prepare for using Azure AD by installing those PowerShell modules.

1. On the **LON-DC1** VM, in Internet Explorer, enter the following URL in the address bar: `http://aka.ms/AA70s3f`

   This will take you to the **Microsoft Download Center** for the **Microsoft Online Services Sign-In Assistant for IT Professionals RTW.**

2. Scroll down on the page and under **Microsoft Online Services Sign-In Assistant for IT Professionals RTW**, verify that English is selected as your **Language,** and then select **Download**.
3. On the **Choose the download you want** page, select the **64 bit** version check box, and then select **Next**.
4. If a notification bar appears at the bottom of the page indicating that Internet Explorer blocked a pop-up from www.microsoft.com, select **Allow once**.
5. In the notification bar that appears at the bottom of the page asking whether you want to Run or Save the setup program from the Download Center, select **Run**.
6. In the **Microsoft Online Services Sign-in Assistant Setup** wizard, select **I accept the terms in the License Agreement and Privacy Statement**, and then select **Install**.
7. On the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, select **Finish**.
8. Close this tab in Internet Explorer.
9. Open **Windows PowerShell** by performing the following steps:
   - Select the magnifying glass (Search Windows) icon on the taskbar at the bottom of the screen and type **powershell** in the Search box that appears.
   - In the menu that appears, right-click on **Windows PowerShell** and select **Run as administrator** in the drop-down menu.
10. In **Windows PowerShell**, type the following command and then press Enter:

    ```
    Install-Module MSOnline
    ```

11. If you are prompted to install the **NuGet provider**, enter **Y** to select [**Y**] **Yes**. Press Enter key.
12. If you are prompted to install the module from **PSGallery,** enter **A** to select [**A**] **Yes to All**. Press Enter key.
13. Once the installation is complete, the screen will return to the Windows PowerShell command prompt.
14. You must then run the following command to install the Azure AD PowerShell module that you just retrieved in the earlier step:

    ```
    Install-Module AzureADPreview
    ```

15. If you are prompted to confirm that you want to execute this command, enter **A** to select [**A**] **Yes to All**.
16. You have now installed the Windows PowerShell modules required to access Azure AD.
17. Remain logged into the domain controller VM and keep the Windows PowerShell window open.

3.0.5 Task 5 - Enable IRM for SharePoint Online

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

Note: While you will validate IRM in Exchange and SharePoint in a later lab, you must enable IRM for SharePoint Online now because it can take up to 60 minutes or more for IRM to show up in SharePoint Online.

By the time you get to the validation exercise in the later lab, IRM should have finished its internal configuration so you won't have to wait for it to be present in SharePoint Online.

1. You should still be logged into your domain controller VM as the **LON-DC1\Admin** account with password: **Pa55w.rd**, and you should still be logged into Microsoft 365 (portal.office.com) as **MOD Administrator**.
2. In the **Microsoft 365 admin center**, scroll down through left navigation pane and under **Admin centers,** select **SharePoint**. This will open the SharePoint admin center.
3. If a **One place for SharePoint administration** pop-up window appears, select **Got it** to close the window.
4. In the **SharePoint admin center**, in the left navigation pane, select **Settings**.
5. At the bottom of the page is a sentence that says **"Can't find the setting you're looking for? Go to the classic settings page."** In this sentence, select the hyperlinked text: **classic settings page**.
6. On the **Settings** page, scroll down to the **Information Rights Management (IRM)** section, select the **Use the IRM service specified in your configuration**, select the **Refresh IRM Settings** button, and then scroll down to the bottom of the page and select **OK**.
7. Do NOT close the SharePoint admin center tab in your Edge browser. Leave your browser open for the next task.

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

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

1. You should still be logged into your domain controller 1 VM as the **LON-DC1\Admin** account, and you should be logged into Microsoft 365 as **MOD Administrator**.
2. In your browser, enter the following URL in the address bar: `https://protection.office.com`.
3. In the **Office 365 Security & Compliance center**, in the left navigation pane, select **Search**, and then under it, select **Audit log search**.
4. In the **Audit log search** window, at the top right of the page, select **Turn on auditing,** and then confirm the **Your organization settings need to be updated. Do you want to continue?** question by selecting **Yes**.
5. Leave the Client 1 VM and the Security and Compliance Center open.

4 End of Lab

5 Module 1 - Lab 1 - Exercise 2 - Manage users and groups

In the following lab exercise, you will take on the role of Holly Dickson, Adatum Corporation's Security Administrator. In this exercise, you will perform several user and group management functions within Microsoft 365. You will create two Office 365 groups and assign existing Microsoft 365 users as members of those groups. You will then delete one of the groups and then use PowerShell to recover the deleted group.

Note: The VM environment provided by your lab hosting provider comes with ten existing Microsoft 365 user accounts, as well as a number of existing on-premises user accounts. Several of these existing user accounts will be used throughout the labs in this course. This will save you from having to perform the tedious task of creating user accounts, which is typically not a task performed by Security Administrators. It will also provide you with the experience of creating a Microsoft 365 user account in case you are not familiar with the process.

5.0.1 Task 2 – Create and Manage Groups

In this task, you will begin implementing Adatum's Microsoft 365 pilot project as Holly Dickson, Adatum's new Security Administrator. Therefore, you will begin this task by logging out of Microsoft 365 as the MOD Administrator and you will log back in as Holly.

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

1. You should still be logged into your domain controller 1 VM as the **LON-DC1\Admin** account, and you should be logged into Microsoft 365 as **MOD Administrator**. On the **Microsoft 365 admin center** tab, select the user icon for the **MOD Administrator** (the **MA** circle) in the upper right corner of your browser, and in the **My account** pane, select **Sign out.**

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

2. In Internet Explorer browser, navigate to `https://portal.office.com/`.
3. In the **Pick an account** window, only the admin account that you just logged out from appears. Select **Use another account**.
4. In the **Sign in** window, enter **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Select **Next**.
5. In the **Enter password** window, enter `Pa55w.rd` and then select **Sign in**.
6. If a **Get your work done with Office 365** window appears, select the **X** to close it.
7. In the **Office 365 home page**, select **Admin** to open the Microsoft 365 admin center (if **Admin** is covered by an **Office 365 apps** box, select **Got it!** to close the box).
8. If a survey window appears, select **Cancel**.
9. In the **Microsoft 365 admin center**, select **Groups** in the left navigation pane, and then under it, select **Active Groups**.
10. In the **Active Groups** page, select **Add a group** that appears on the menu bar above the list of groups.
11. In the **Choose a group type** window, select **Microsoft 365 (recommended)** and then select **Next**.
12. In the **Set up the basics** window, enter `Inside Sales` in the **Name** field, and then enter `Collaboration group for the Inside Sales team.` in the **Description** field. Select **Next**.
13. In the **Assign Owners** window, 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**.
14. In the **Edit settings** window, enter `insidesales` in the **Group email address** field. Under the **Privacy** section, verify the **Public** option is selected (select it if need be), and under the **Add Microsoft Teams to your group** section, verify the **Create a team for this group** checkbox is selected (select it if need be). Select **Next**.
15. In the **Review and finish adding group** window, 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).
16. On the **New group created** window, note the comment at the top of the page that it may take 5 minutes for the new group to appear in the list of groups.

    Select **Close**. This returns you to the **Groups** page.

17. Repeat steps 10-16 to add a new group with the following information:
    - Group type: `Security`
    - Name: `IT Admins`
    - Description: `IT administrative personnel`

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

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

    Note: The IT admins group does not have a group email address because it's a Security group. Two additional group types are Mail-enabled Security groups and Distribution groups. We did not use either of these group types in this lab because it can take up to an hour for these two types of groups to appear in the Groups list; whereas, Office 365 groups and Security groups usually take just a matter of minutes to appear.

19. You're now ready to add members to the groups. In the list of **Groups**, select the **Inside Sales** group, which opens a window for the group.
20. In the **Inside Sales** group window, select the **Members** tab.
21. Under the **Members** section, you can see the two owners (Allan and Patti), but you can also see that there are zero (0) members. Select **View all and manage members** to add members to the group.
22. In the **Inside Sales** group window, select **+ Add members**. This displays the list of current users.
23. In the list of users, select **Diego Siciliani** and **Lynne Robbins**, and then scroll to the bottom and select **Add (2)**.
24. Select **Back arrow**.
25. On the **Inside Sales** window, Diego and Lynne should now appear as members of the group. Select the **X** in the upper right corner to close the window.
26. Repeat steps 19-25 to add **Isaiah Langer**, **Megan Bowen**, and **Nestor Wilke** as members of the **IT admins** group.
27. You now want to test the effect of deleting a group. In the list of **Groups,** select the vertical ellipsis icon (**More actions**) that appears to the right of the **Inside Sales** group. In the menu box that appears, select **Delete group**.
28. In the **Delete Inside Sales** window, select the **Delete group** button.
29. Once the group is deleted, select **Close**.
30. This will return you to the list of **Groups** in the **Microsoft 365 admin center**. The **Inside Sales** group should no longer appear. If the Inside Sales group still displays, wait a couple of minutes and then select the **Refresh** option on the menu bar. The updated **Groups** list should no longer include the Inside Sales group.
31. To verify whether deleting this group affected any of its owners or members, select **Users** and then **Active Users** in the left navigation pane.
32. In the **Active users** list verify that the two owners (**Allan Deyoung** and **Patti Fernandez**) and the two members (**Diego Siciliani** and **Lynne Robbins**) of the Inside Sales group still appear in the list of users. This verifies that deleting a group does not delete the user accounts that were owners or members of the group.
33. Remain logged into the domain controller VM with the Microsoft 365 admin center open in your browser for the next task.

5.0.2 Task 3 – Recover Groups using PowerShell

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

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

1. If you're not logged into the **LON-DC1** VM as **ADATUM\Administrator** and password **Pa55w.rd**, then please do so now.
2. If Windows PowerShell is still open from the previous exercise, select the **Windows PowerShell** icon on the taskbar; otherwise, you must open an elevated instance of Windows PowerShell just as you did before. Maximize your PowerShell window.
3. In **Windows PowerShell**, type the following commands (press Enter after each command):

- You must run the following command to connect with an authenticated account to use Active Directory cmdlet requests:

  ```
  Connect-AzureAD
  ```

- A new window will appear requesting your credentials. Sign in using Holy's Microsoft 365 account of **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and **Pa55w.rd** as the Password.

- You should then run the following command to display the repository of deleted groups (this should display the **Inside Sales** group that you earlier deleted):

  ```
  Get-AzureADMSDeletedGroup
  ```

- Before you can restore this deleted group, you must first copy the Object ID of the Inside Sales group that appears in the table of deleted groups. When you perform the next command to restore the group, you will use this ID to identify the group that you want restored.

  To copy the ID, select the entire ID and then press Ctrl-C.

- You should then run the following command to retrieve and restore the deleted group whose Object ID matches the value you enter:

  Note: Replace the {objectId} in the following command with the ID number for the Inside Sales group that you copied in the prior step. When you enter the following Restore command and you get to the point of pasting in the {objectId} parameter, press Ctrl-V to paste in the Id. Then press Enter to run the command. **NOTE:** If nothing happens when you hit Enter, then extraneous hidden characters may have been pasted in following the object ID. If this occurs, retype the command and hit the Delete key a couple of times after pressing Ctrl-V, and then press Enter again.

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

4. Leave your Windows PowerShell window open for the next exercise; simply minimize the PowerShell window for now.
5. You should now validate that the **Inside Sales** group has been recovered. To do this, go to the **Microsoft 365 Admin Center** in your Internet Explorer browser, select **Groups** from the left-hand navigation pane, and then under it select **Active Groups** to display the list of groups.
6. Verify that the **Inside Sales** group has been restored and is present in the list of groups. If the Inside Sales group does not appear, wait a minute or two and then select the **Refresh** icon to the right of the URL in Internet Explorer.
7. You now want to verify that the recovery process correctly updated the group's membership. From the **Groups** windows, select the **Inside Sales** group.
8. In the **Inside Sales** window, select the **Members** tab. **Allan Deyoung** and **Patti Fernandez** should appear as owners of the group, and **Diego Siciliani** and **Lynne Robbins** should appear as members of the group.
9. Close the **Inside Sales** window.
10. Leave your browser windows open so that they're ready for the next task.

6 End lab

7 Module 1 - Lab 2 - Exercise 1 - Configure Self-service password reset (SSPR) for user accounts in Azure AD

7.0.1 Scenario

The Help Desk has indicated that a large number of support tickets are related to password resets. You have been asked to setup a way for users to reset their password on their own.

7.0.1.1 Task 1: Enable self-service password reset

1. Switch to **LON-CL1** and sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

2. On the task bar select **Microsoft Edge**, open Azure by going to `https:/portal.azure.com/`. Login as Holly Dickson from the previous lab. Navigate to **Azure Active Directory**
3. In the navigation pane under **Manage** select **Users**, then select **Password reset**.
4. In the **Password reset | Properties** window, select **All** to enable self-service password reset to all users. Select **Save**.
5. On the **Password reset | Properties** blade, select **Authentication methods**.
6. For the methods available to users, ensure that **Mobile Phone (SMS only)** and **Email** are selected, and then select **Security Questions**.
7. For the **Number of questions required to register**, select **3**.
8. For the **Number of questions required to reset**, select **3**.
9. In the **Select security questions** section, select **No security questions configured**, then select **Predefined**. Select three questions of your choice, and then select **OK** twice.
10. Select **Save**.
11. Select **Registration** Select **No** for **Require users to register when signing in**, and the select **Save**.

7.0.1.2 Task 2: Register user for self-service password reset

With SSPR enabled and configured, test the SSPR process with a user that's part of the group you selected in the previous section, such as Test-SSPR-Group. In the following example, the testuser account is used. Provide your user account that's part of the group you enabled for SSPR in the first section of this mini-lab.

> **Note** When you test the self-service password reset, use a non-administrator account. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password.

1. In your web browser at the upper right corner of the page, select your account name, and then select **Sign in with a different account**.
2. Sign in as **AllanD@yourtenant.onmicrosoft.com** with the password that was assigned by your lab hosting service.
3. Browse to the self service password registration page at https://aka.ms/ssprsetup.
4. On the **Security info** page, click **Add method**. Select your desired authentication method such as **Phone** and proceed through the setup steps.

   > **Note** If prompted to use an email you will need to use an e-mail address other than the tenant domain provided for this lab. If one is not available, you can skip the e-mail verification and continue with the next step. Sign in to your email account, read the code, type it in the verification field, and then select **Verify**.

   > **Note** If you don't find a message with a code in your inbox, check the junk folder.

7.0.1.3 Task 3: Test self-service password reset

1. Go to `https://aka.ms/sspr` and enter the username for Alan (**AllanD@yourtenant.onmicrosoft.com**). Complete the Captcha below and click **Next**.
2. Request verification using the method that you configured in the previous task.
3. Enter the verification code you received and then click **Next**.
4. Enter a **new password** and click **Finish**.

8 Continue to Exercise 2

9 Module 1 - Lab 2 - Exercise 2 - Deploy Azure AD Smart Lockout

Adatum's CTO has asked you to deploy Azure AD Smart Lockout, which assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get admitted into your network. Smart

Lockout can recognize sign-ins coming from valid users and treat them differently than sign-ins from attackers and other unknown sources.

The CTO is anxious to implement Smart Lockout because it will lock out the attackers while letting Adatum's users continue to access their accounts and be productive. The CTO has asked you to configure Smart Lockout so that users can't use the same password more than once, and they can't use passwords that you deem too simplistic or common.

1. On the Domain Controller (**LON-DC1**), select the **Server Manager** icon on the taskbar if it's already open; otherwise, open it now.
2. In **Server Manager**, select **Tools** in the upper-right menu bar, and in the drop-down menu, select **Group Policy Management.**
3. Maximize the **Group Policy Management** window, if necessary.
4. You want to edit the group policy that includes your organization's account lockout policy. If necessary, in the root console tree, expand **Forest:Adatum.com**, then expand **domains**, and then expand **Adatum.com**.

Under **Adatum.com**, right-click on **Default Domain Policy** and then select **Edit** in the menu.

5. Maximize the **Group Policy Management Editor** window.
6. In the **Default Domain Policy** tree in the right pane, browse to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies.**
7. In the **Account Policies** folder, select **Account Lockout Policy**.
8. As you can see in the right pane, none of the smart lockout parameters have been defined. You are going to use the **Azure AD admin center** to assign these values.

In **Internet Explorer**, open a new browser tab and go to `https://portal.azure.com`. Sign-in as Holly Dickson if you are not already signed in on another browswer tab. Search for **Azure Active Directory** and click **Azure Active Directory**.

10. In the **Adatum Corporation | Overview** page, in the middle navigation pane under the **Manage** section, scroll down and select **Security**.
11. In the **Security | Getting started** window, in the middle pane under the **Manage** section, select **Authentication Methods**.
12. In the **Authentication methods | Authentication method policy (Preview)** page, in the middle pane under the **Manage** section, select **Password protection.**
13. In the **Authentication methods | Password protection** window, in the detail pane on the right, enter the following information:
    - In the **Custom smart lockout** section:
        - **Lockout threshold:** this field indicates how many failed sign-ins are allowed on an account before its first lockout. The default is 10. For testing purposes, Adatum has requested that you set this to `3`.
        - **Lockout duration in seconds:** This is the length in seconds of each lockout. The default is 60 seconds (one minute). Adatum has requested that you change this to `90` seconds.
    - In the **Custom banned passwords** section:
        - **Enforce custom list**: select **Yes**
        - **Custom banned password list:** Enter the following values (press Enter after entering each value so that each value is on a separate line):
            - `Password01`
            - `F00tball01`
            - `Se@Hawks1`
            - `Never4get!!`
14. Select **Save** on the menu bar at the top of the page.

15. You should now test the banned password functionality. Select Holly Dicksons's user icon in the upper right corner of the screen and click **View account**, and in the menu that appears select **Change password**.
16. A new tab will open displaying the **change password** window. Enter `Pa55w.rd` in the **Old password** field, enter `Never4get!!` in the **Create new password** and **Confirm new password** fields, and then select **submit**. Note the error message that you receive.
17. In your browser, close the **Change password** tab.
18. You should now test the lockout threshold functionality. In the **My Dashboard - Azure Active Directory admin center** tab, select Holly Dicksons's user icon in the upper right corner of the screen, and in the menu that appears select **Sign out**.
19. Once you are signed out as Holly, the **Pick an account** window will appear. Select **Use another account**.
20. In the **Sign in** window, enter **AllanD@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is the tenant suffix ID assigned to you by your lab hosting provider), and then select **Next**.
21. On the **Enter password** window, enter any mix of letters and then select **Sign in**. Note the invalid password error message. Repeat this step 2 more times. Since you set the **Lockout threshold** to **3**, note the error message that you receive after the third attempt. Allan's account has been temporarily locked to prevent unauthorized access.

    Note: You will be prohibited from logging in as Allan until after the **90 second lockout duration** that you set earlier.
22. After 90 seconds, try logging in again to verify that you can log in.

10 End of lab.

11 Module 2 - Lab 1 - Exercise 1 - Setting up your organization for identity synchronization

You are Holly Dickson the security administrator for Adatum Corporation, and you have Microsoft 365 deployed in a virtualized lab environment. In this lab, you will implement identity synchronization between your Microsoft 365 tenant accounts and your local active directory accounts.

11.0.1 Task 1 - Configure your UPN suffix

1. On LON-DC1, log on as **Adatum\Administrator** and password assigned from your lab hoster.
2. Using Windows PowerShell as administrator, update the UPN suffix for the domain and on the UPN on every user in AD DS with "@zzzzzzz.onmicrosoft.com" (where zzzzzzz is your unique UPN name) for the domain name. To do this, run the following command (remember to change zzzzzzz to your unique UPN name):

   ```
   Set-ADForest -identity "adatum.com" -UPNSuffixes @{replace="zzzzzzz.onmicrosoft.com"}
   ```
3. Next type the follow command (remember to change zzzzzzz to your unique UPN name):

   ```
   Get-ADUser -Filter * -Properties SamAccountName | ForEach-Object { Set-ADUser $_ -UserPrincipalName
   ```
4. At the Windows PowerShell prompt, type the following command, and then press Enter:

   ```
   Set-ExecutionPolicy Unrestricted
   ```
5. To confirm the execution policy change, enter **A** for Yes to All press Enter key.

11.0.2 Task 2 - Enable Directory Synchronization

1. Open your browser and go to `https://portal.office.com/`
2. Sign in as **holly@M365xZZZZZZ.onmicrosoft.com** with the password `Pa55w.rd`.
3. Click **Admin** to go to the Microsoft 365 admin center.
4. If asked about **update your admin contact information **click the Cancel button to skip this request. **Note:** If you see the Active Directory synchronization is being activated warning, you can ignore it at this time, but you will not be able to run directory synchronization later in this exercise. You must wait

until directory synchronization is activated. However, you can complete the following steps, even if you do see the warning message.

5. In the left navigation, select **users** icon and select **Active users**, click on the ellipses at the top menu and choose **Directory Synchronization**.
6. Click on the **Go to the Download center to get the Azure AD Connect tool**. Download and Run the download once prompted.

11.0.3 Task 3 - Run Azure AD Connect

1. On the Microsoft Azure Active Directory Connect setup wizard, proceed through the wizard.
2. Agree to the license terms and privacy notice.
3. Click on **Use express settings**.
4. On the **Connect to Azure AD** screen enter your Office 365 admin username of **holly@M365xZZZZZZ.onmicrosoft.com** with password `Pa55w.rd` and click Next.
5. On the **Connect to AD DS** screen enter your domain administrator **ADATUM\Administrator** and password `Pa55w.rd` and select **Next**.
6. Select **Continue without matching all UPN suffixes to verified domains** checkbox. Select **Next** on the Azure AD sign-in configuration screen.
7. On the **Ready to configure** screen make sure the check box for **Start the synchronization process when configuration completes** is marked and select **Install**.
8. Wait for the installation to complete (this may take several minutes).
9. Select **Exit**.

11.0.4 Task 4 - Validate the results of directory synchronization and license a user.

1. To verify the new user you created open the Office 365 Admin Center in the browser by typing `https://portal.office.com` in the address bar.
2. Sign in as Holly Dickson with the following credentials: User name: **holly@M365xZZZZZZ.onmicrosoft.com**, Password: `Pa55w.rd`
3. Navigate to the **Active Users**.
4. You should now see many users that have become synced from the local Active Directory. You may need to click the refresh button to update the data in the page. Select Abbie Parsons. Abbie is a user that was only in the AD DS domain prior to our synchronization.
5. Edit Abbie Parsons Product licenses as follows:
   - Location = United Kingdom
   - Product License = Enterprise Mobility + Security E5
6. Click **Save changes** to make the changes. Close the window.

You have successfully synced local ADATUM users into Office 365 and licensed the synced user Abbie Parsons.

12 End of lab

13 Module 3 - Lab 1 - Exercise 1 - MFA Authentication Pilot (Require MFA for specific apps with Azure Active Directory conditional access)

13.0.1 Task 1: Create your conditional access policy

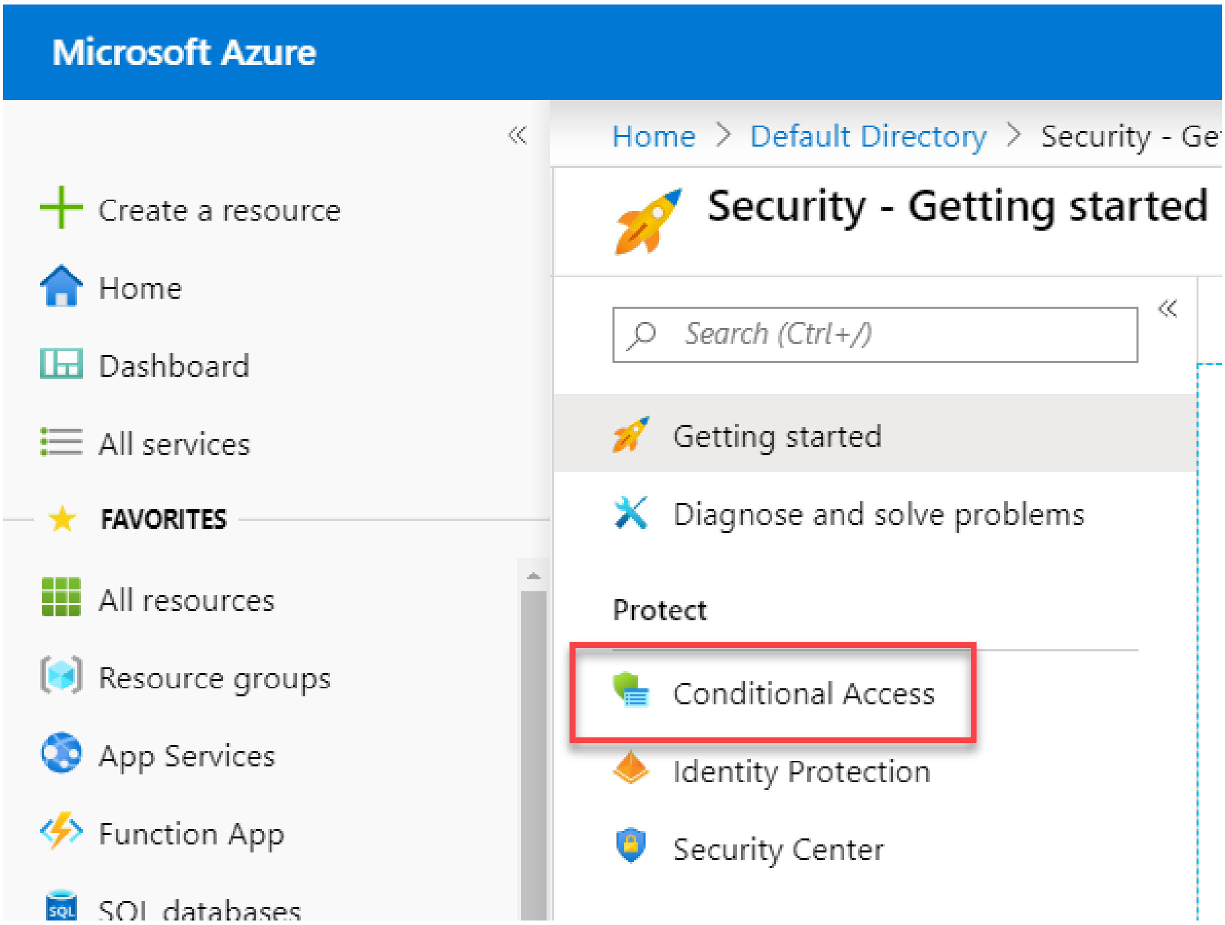
This lab shows how to create the required conditional access policy to require MFA for certain users. The scenario uses:

- The Azure portal as placeholder for a cloud app that requires MFA.
- Your sample user to test the conditional access policy.

In your policy, set:

Setting	Value
Users and groups	Patti Fernandez
Cloud apps	Microsoft Azure Management
Grant access	Require multi-factor authentication

1. Sign in to the Azure Portal `https://portal.azure.com` as Holly Dickson with password: `Pa55w.rd`.
2. In the Azure portal, on the hub menu go to **Azure Active Directory** by using More Services to search if necessary.
3. On the left click **Security** and then select **Conditional Access**.



4. On the **Conditional Access** page, in the toolbar on the top, click **New Policy**.

   Note: if this is greyed out, refresh the browser session.
5. On the **New** page, in the **Name** textbox, type `Require MFA for Azure portal access`.
6. In the **Assignment** section, click **Users and groups**.
7. On the **Users and groups** page, perform the following steps:

   a. Click **Select users and groups**, and then select **Users and groups**.

   b. Click **Select**.

   c. On the **Select** page, select `Patti Fernandez`, and then click **Select**.
8. Back on the New page click **Cloud apps or actions**.
9. On the **Cloud apps or actions** page, perform the following steps:

   a. Click **Select apps**.

   b. Click **Select**.

   c. On the **Select** page, select **Microsoft Azure Management**, and then click **Select**.
10. In the **Access controls** section, click **Grant**.
11. On the **Grant** page, perform the following steps:
    1. Select **Grant access**.
    2. Select **Require multi-factor authentication**.
    3. Click **Select**.

12. In the **Enable policy** section, click **On**.
13. Click **Create**.

```
**Note:** If the policy fails check your work and **Create** again.
```

13.0.2 Task 2: Evaluate a simulated sign-in

Now that you have configured your conditional access policy, you probably want to know whether it works as expected. As a first step, use the conditional access what if policy tool to simulate a sign-in of your test user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report.

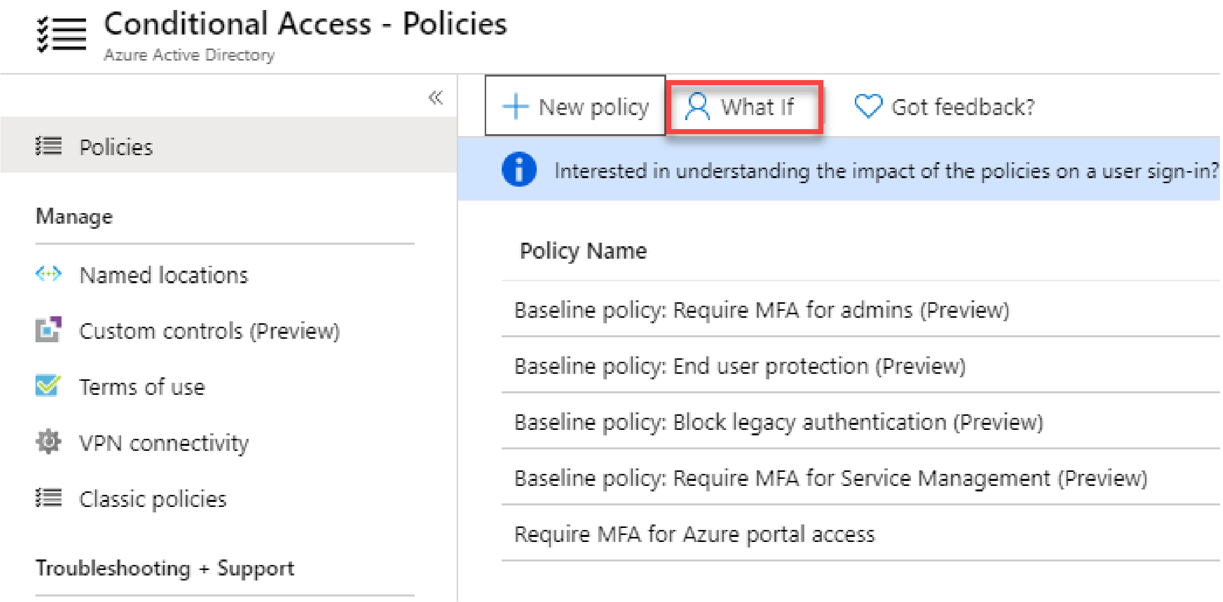
We will initialize the what if policy evaluation tool for:

- **Patti Fernandez** as user
- **Microsoft Azure Management** as cloud app

Clicking **What If** creates a simulation report that shows:

- **Require MFA for Azure portal access** under **Policies that will apply**
- **Require multi-factor authentication** as **Grant Controls**.

1. On the Conditional access - Policies page, in the menu on the top, click **What If**.



Interested in understanding the impact of the policies on a user sign-in?

Policy Name
Baseline policy: Require MFA for admins (Preview)
Baseline policy: End user protection (Preview)
Baseline policy: Block legacy authentication (Preview)
Baseline policy: Require MFA for Service Management (Preview)
Require MFA for Azure portal access

2. Click **Users**, select `Patti Fernandez`, and then click **Select**.
3. To select a cloud app, perform the following steps:

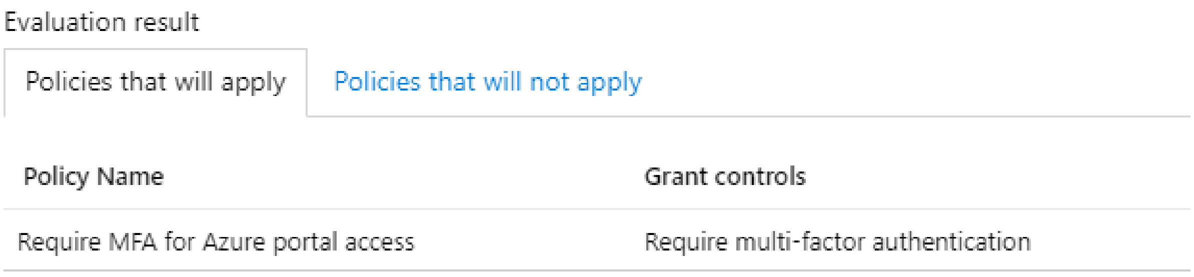
   a. Select **Cloud apps or actions**.

   b. On the **Cloud apps or actions page**, select **Select apps**.

   c. Click **Select**.

   d. On the **Select** page, select **Microsoft Azure Management**, and then click **Select**.

   e. On the cloud apps or actions page, select **Done**.
4. In the What If page select **What If**.
5. Note the result, Require MFA for Azure portal access.



Evaluation result

Policies that will apply | Policies that will not apply

Policy Name	Grant controls
Require MFA for Azure portal access	Require multi-factor authentication

13.0.3 Task 3: Test your conditional access policy

In the previous section, you have learned how to evaluate a simulated sign-in. In addition to a simulation, you should also test your conditional access policy to ensure that it works as expected.

To test your policy, open an in-private browsing session and try to sign-in to the Azure portal `https://portal.azure.com` using your **Patti Fernandez** account. You should see a dialog that requires you to set your account up for additional security verification.

13.1 Continue to exercise 2.

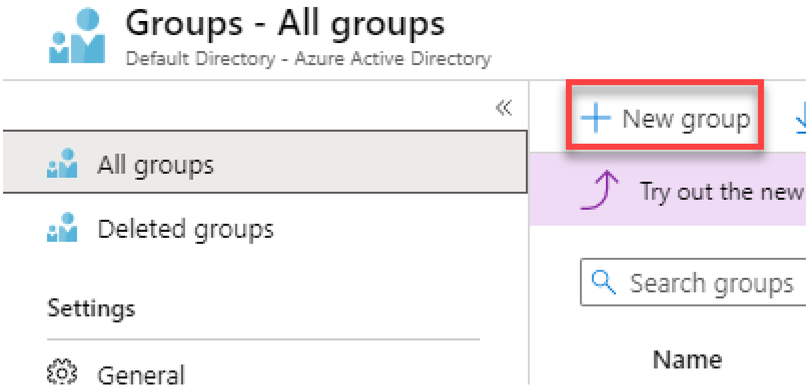
14 Module 3 - Lab 1 - Exercise 2 - MFA Conditional Access (Complete an Azure Multi-Factor Authentication pilot roll out)

In this exercise you will configure a conditional access policy enabling Azure Multi-Factor Authentication (Azure MFA) when logging in to the Azure portal. The policy is deployed to and tested on a specific group of pilot users. Deployment of Azure MFA using conditional access provides significant flexibility for organizations and administrators compared to the traditional enforced method.

- Enable Azure Multi-Factor Authentication
- Test Azure Multi-Factor Authentication

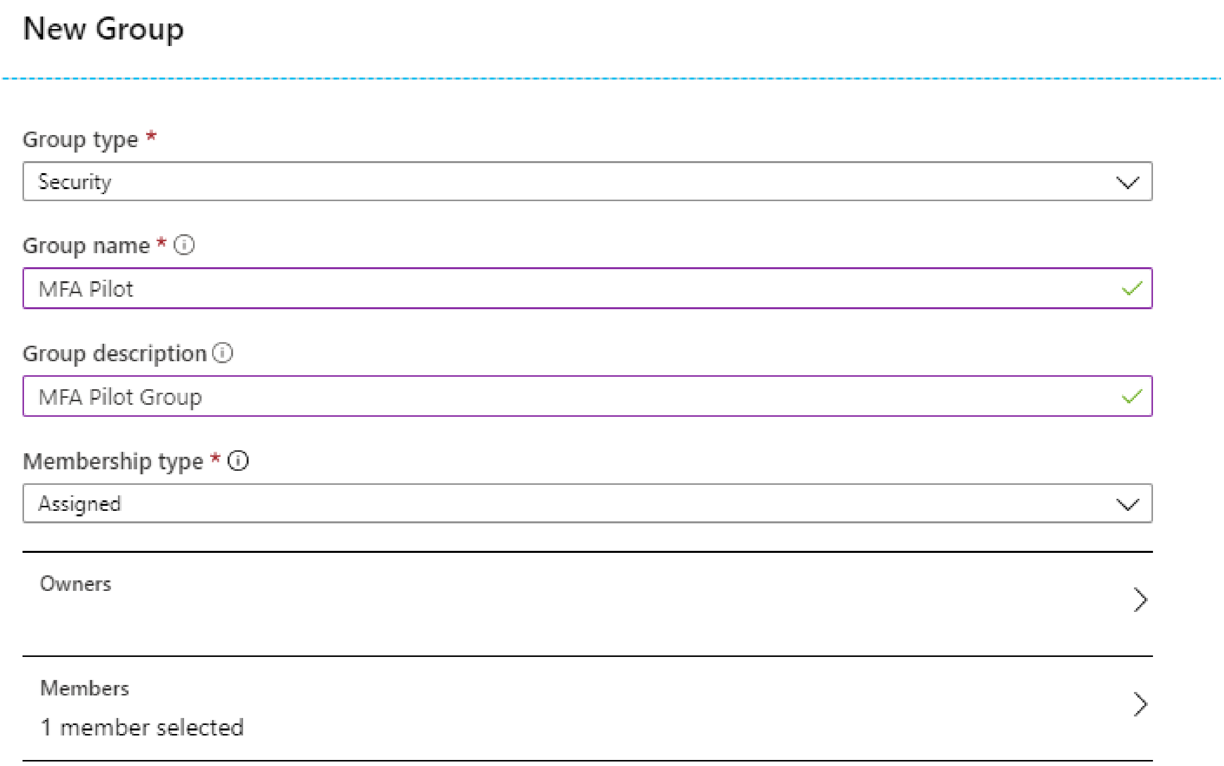
14.0.1 Task 1: Enable Azure Multi-Factor Authentication

1. Return to the the Azure portal that is logged in as your Global Admin Holly Dickson.
2. On the Hub go to **Azure Active Directory**,
3. Click **Groups** and click + **New group**.



4. Enter the following information then select **Create**:

   - Group type; `Security`
   - Group Name: `MFA Pilot`
   - Group description: `MFA Pilot Group`
   - Membership type: `Assigned`
   - Members: Select `Lynne Robbins`



New Group

Group type *
Security

Group name *
MFA Pilot

Group description
MFA Pilot Group

Membership type *
Assigned

Owners

Members
1 member selected

5. Browse to **Azure Active Directory**, click **Security** and select **Conditional access** on the **Protect** Blade.
6. Select + **New policy**
7. Name your policy `MFA Pilot`
8. Click **users and groups**, select the **Select users and groups** radio button. Check the box for **Users and groups** and click **Select**.
   - Select your pilot group `MFA Pilot`
   - Click **Select**
9. Click **Cloud apps or actions**, select the **Select apps** radio button.
   - Click **Select**. The cloud app for the Azure portal is `Microsoft Azure Management` select it.
   - Click **Select**
10. Skip the **Conditions** section
11. Click **Grant**, make sure the **Grant access** radio button is selected
    - Check the box for **Require multi-factor authentication**
    - Click **Select**
12. Skip the **Session** section
13. Set the **Enable policy** toggle to **On**
14. Click **Create**

    Note: If the policy fails check your work and **Create** again.

14.0.2 Task 2: Test Azure Multi-Factor Authentication

To prove that your conditional access policy works, you test logging in to a resource that should not require MFA and then to the Azure portal that requires MFA.

2. Open a new browser window in InPrivate or incognito mode and browse to **`https://portal.azure.com`**
   - Log in with the Lynne Robbins user (Lynne's password is likely the same as the MOD Administrator password provided by your lab hoster) and note that you should now be required to register for and use Azure Multi-Factor Authentication.
   - Close the browser window.

15 End of lab

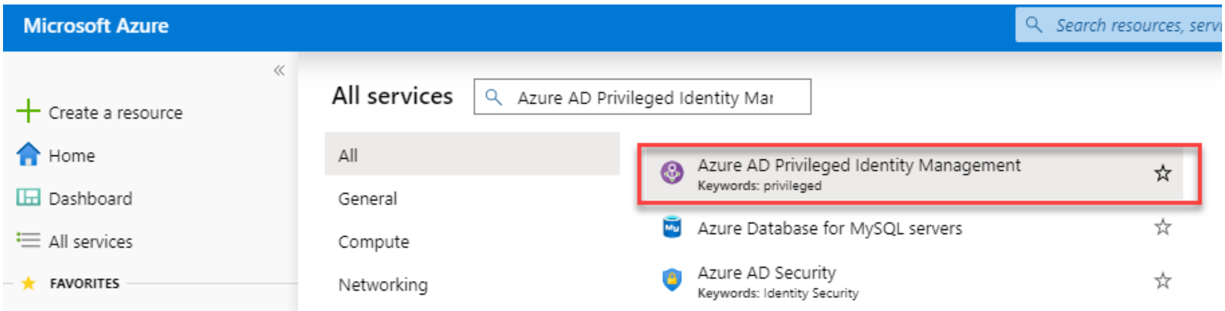
16 Module 3 - Lab 2 - Exercise 1 - Manage Azure Resources

Scenario

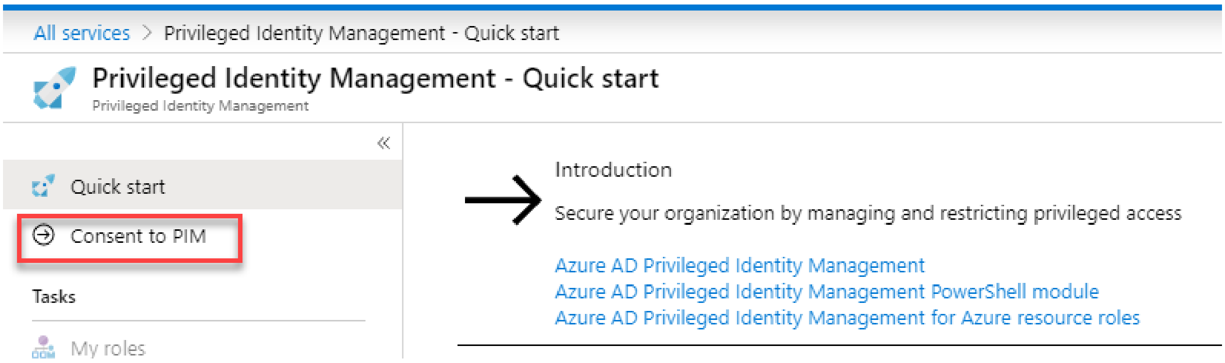
In this lab, you will learn how to use Azure Privileged Identity Management (PIM) to enable just-in-time administration and control the number of users who can perform privileged operations. You will also learn about the different directory roles available as well as newer functionality that includes PIM being expanded to role assignments at the resource level.

16.0.1 Task 1: Discover resources

1. If you are still logged into the Microsoft 365 admin center as MOD Adminsitrator switch users to Holly Dickson. Go to the **Azure Portal** `https://portal.azure.com/` and sign in as Global Administrator Holly Dickson, click **All services** then search for and select `Azure AD Privileged Identity Management`.



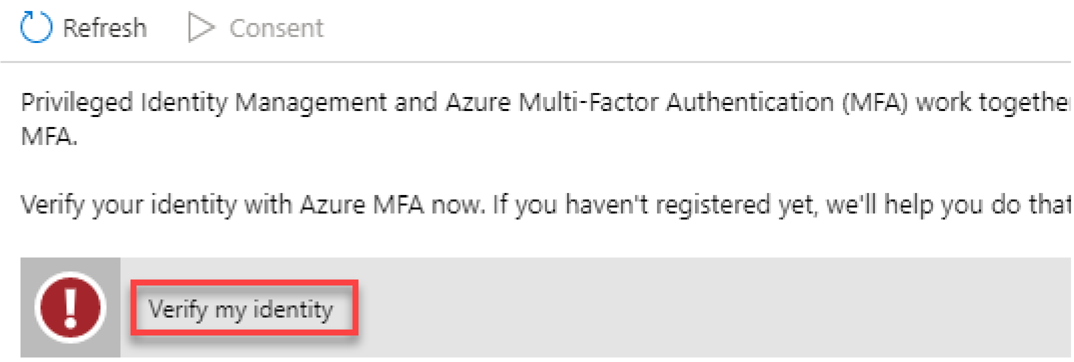
2. Click consent to PIM if it appears. In some tenants PIM is already enabled and therefore these steps are unnecessary.


All services > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Privileged Identity Management
Quick start
Consent to PIM
Tasks
My roles
Introduction

Secure your organization by managing and restricting privileged access

Azure AD Privileged Identity Management
Azure AD Privileged Identity Management PowerShell module
Azure AD Privileged Identity Management for Azure resource roles

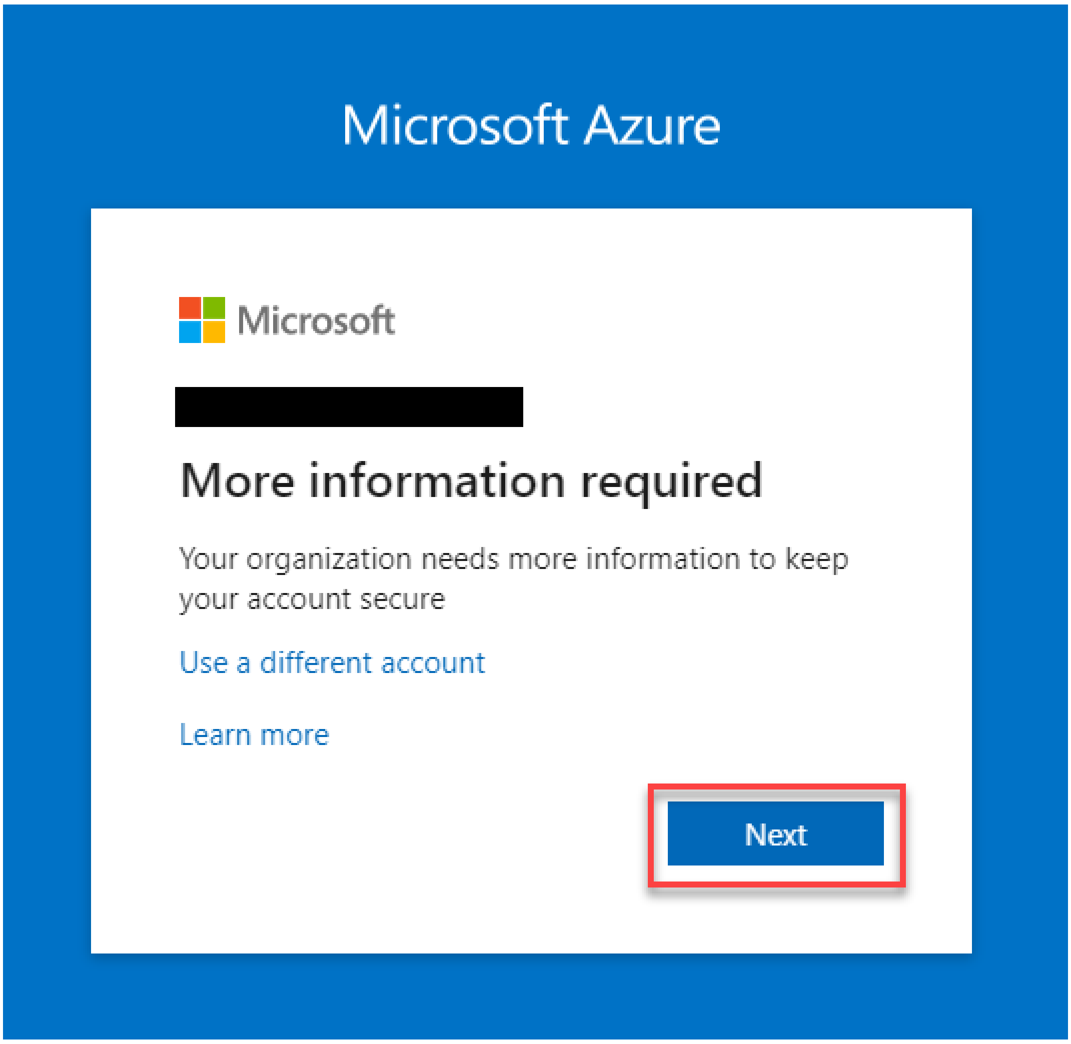
3. Click **Verify my identity** if it appears.



Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work togethe
MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that

4. Click **Next**.



Microsoft Azure

Microsoft

[redacted]

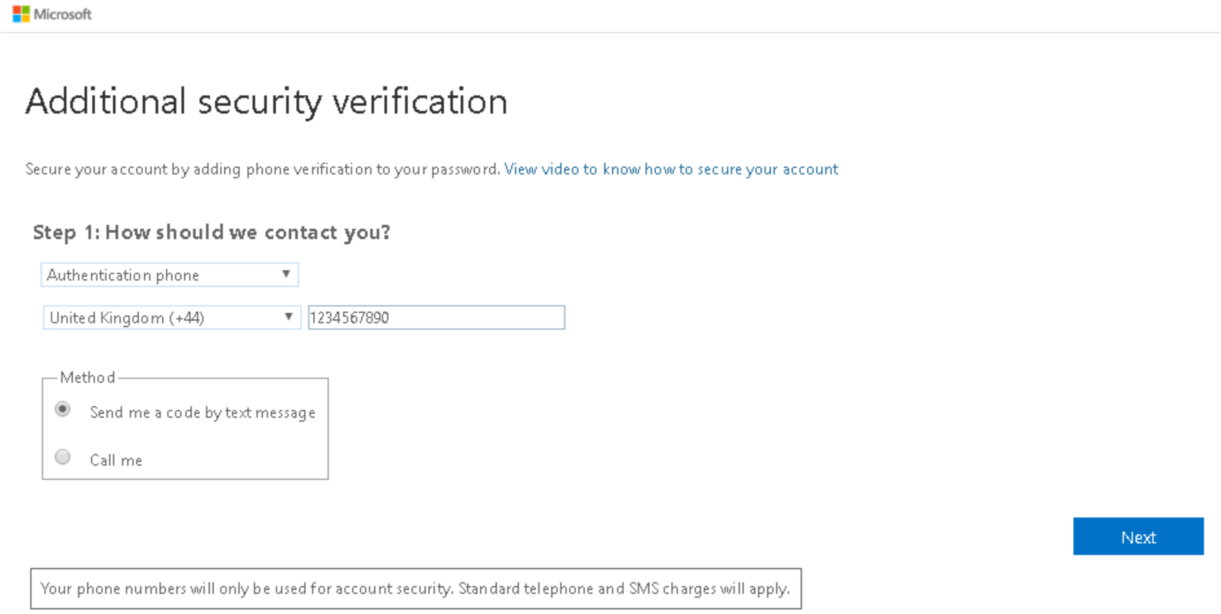
More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

5. Enter your mobile/cell phone details and click **Next**.



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone ▾

United Kingdom (+44) ▾ 1234567890

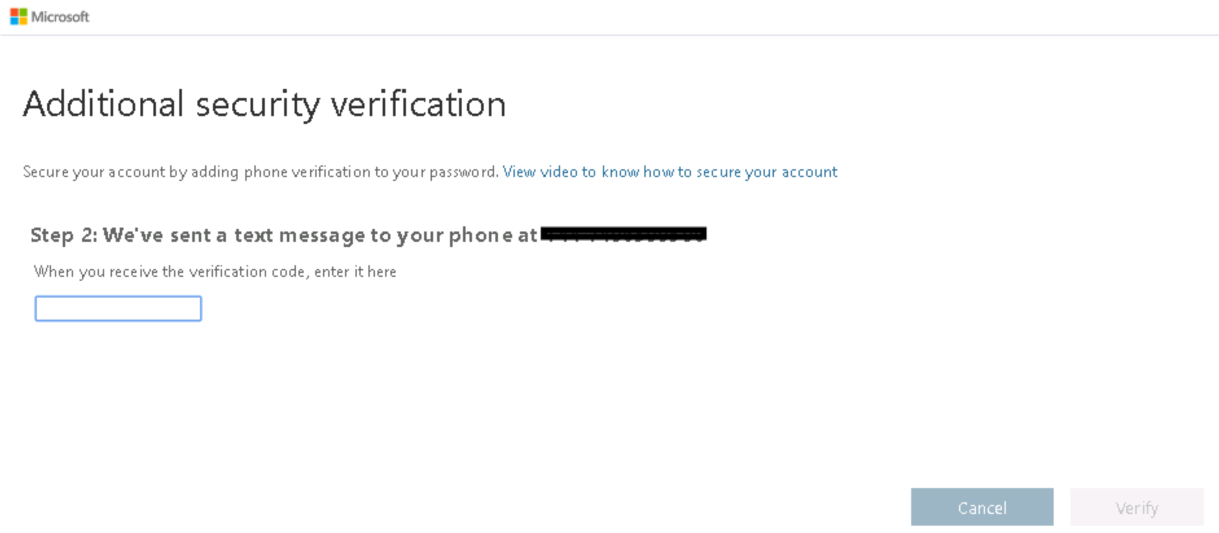
Method

● Send me a code by text message

○ Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

6. Enter the code when you receive it via SMS and click **Verify**.



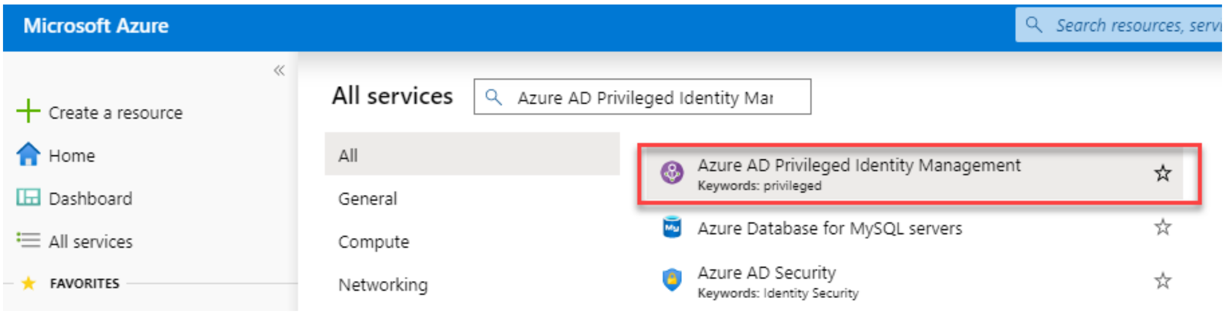
Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

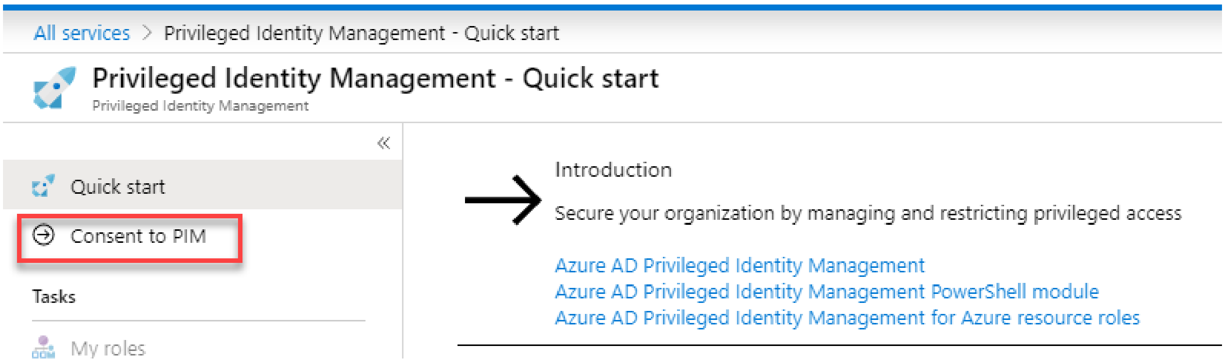
Step 2: We've sent a text message to your phone at [redacted]

When you receive the verification code, enter it here

7. Once the verification is successful, click **Done**.
8. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.

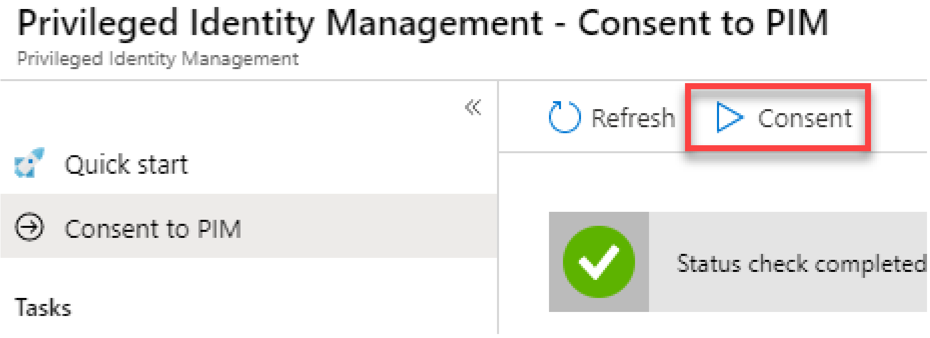


9. Click consent to PIM if it appears.


All services > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Privileged Identity Management
Quick start
Consent to PIM
Tasks
My roles
Introduction
Azure AD Privileged Identity Management
Azure AD Privileged Identity Management PowerShell module
Azure AD Privileged Identity Management for Azure resource roles

Secure your organization by managing and restricting privileged access

10. Back on the **Consent to PIM blade** click **Consent** and click **Yes**.


Privileged Identity Management - Consent to PIM
Privileged Identity Management
Quick start
Consent to PIM
Tasks
Refresh
Consent

Status check completed

11. Refresh the Azure Portal by pressing **F5**.

Note: If by refreshing the portal in the browser does not display PIM as being enabled then log out and back into the Azure Portal.

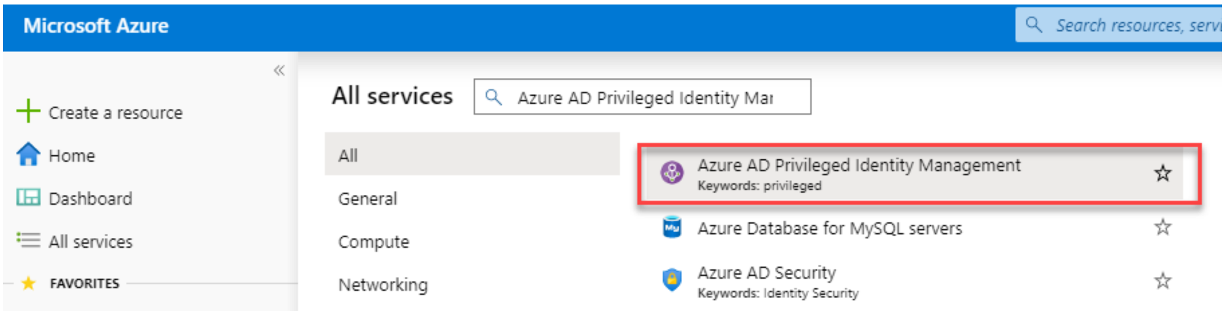
17 Continue to exercise 2

18 Module 3 - Lab 2 - Exercise 2 - Assign Directory Roles

18.0.1 Task 1: Make a user eligible for a role

In the following task you will make a user eligible for an Azure AD directory role.

1. Sign in to Azure portal
2. In the Azure Portal, click **All services** and search for and select `Azure AD Privileged Identity Management`.



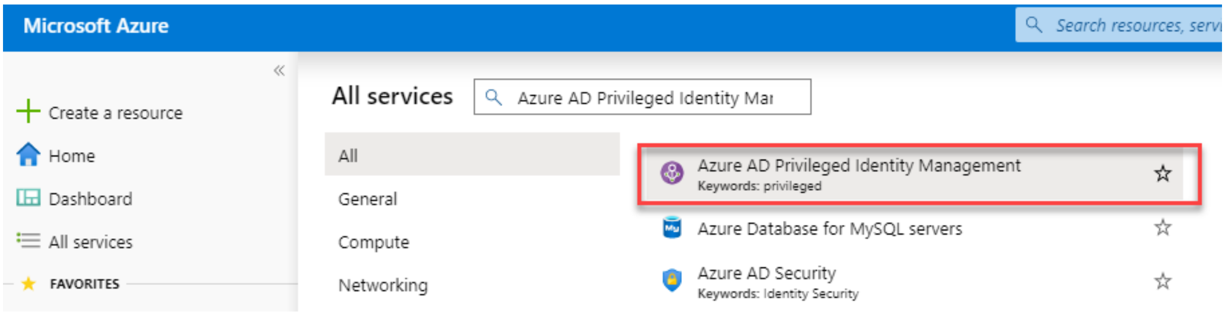
All services: Azure AD Privileged Identity Mar

3. Select **Roles**. If this is option is still greyed you may need to refresh your browser.
4. Select `Billing Administrator`.
5. Select + **Add assignments** to open Select a member. In the Add assignments screen click **No member selected**.
6. In the **Select a member screen** select `Patti Fernandez` and then click **Select**.
7. In Add assignments screen on the Setting tab uncheck the **Permanently eligible** checkbox. Click **Assign**. Review the added member in the assignment window.
8. When the role is assigned, the user you selected will appear in the members list as **Eligible** for the role.

18.0.2 Task 2: Make a role assignment permanent

Follow these steps if you want to make a role assignment permanent.

1. In the Azure Portal, click **All services** and search for and select `Azure AD Privileged Identity Management`.



All services: Azure AD Privileged Identity Mar

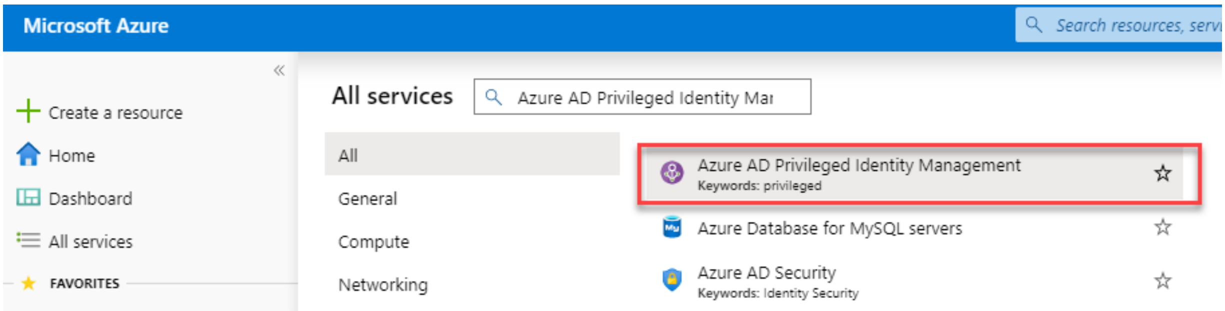
2. Click **Azure AD roles**.
3. Click **Assignments**.
4. Click **Update** for Patti as Billing Administrator and then mark the **Permanently eligble** box. In Membership settings click **Save**.

Results: The Billing Administrator role is now listed as **permanent** for Patti Fernandez. In other words Patti is permanently eligible to be elevated to the Billing Administrator role.

18.0.3 Task 3: Remove a user from a role

You can remove users from role assignments, but make sure there is always at least one user who is a permanent Global Administrator.

1. In the Azure Portal, click **All services** and search for and select `Azure AD Privileged Identity Management`.



2. Click **Azure AD roles**.
3. Click **Assignments**.
4. Use the Member filter to again select Patti Fernandez.
5. In the Action area under Eligible assignments click **Remove**.
6. In the message that asks you to confirm, click **Yes**. The role assignment will be removed.

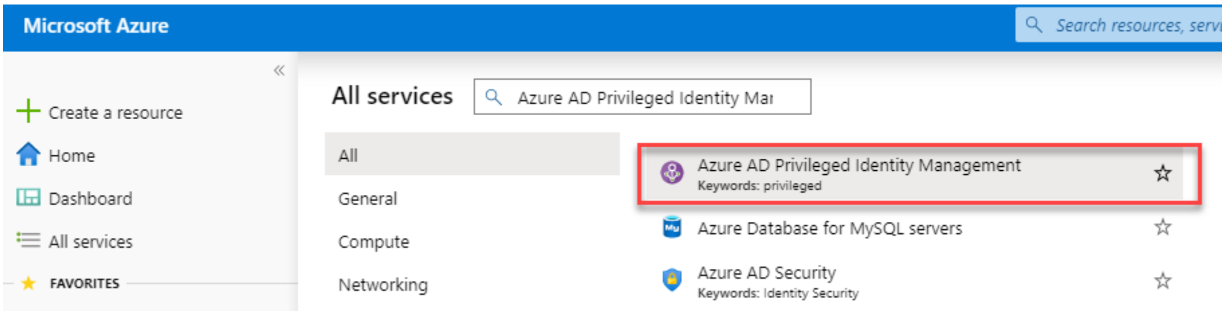
19 Continue to exercise 3

20 Module 3 - Lab 2 - Exercise 3 - Activate and Deactivate PIM Roles

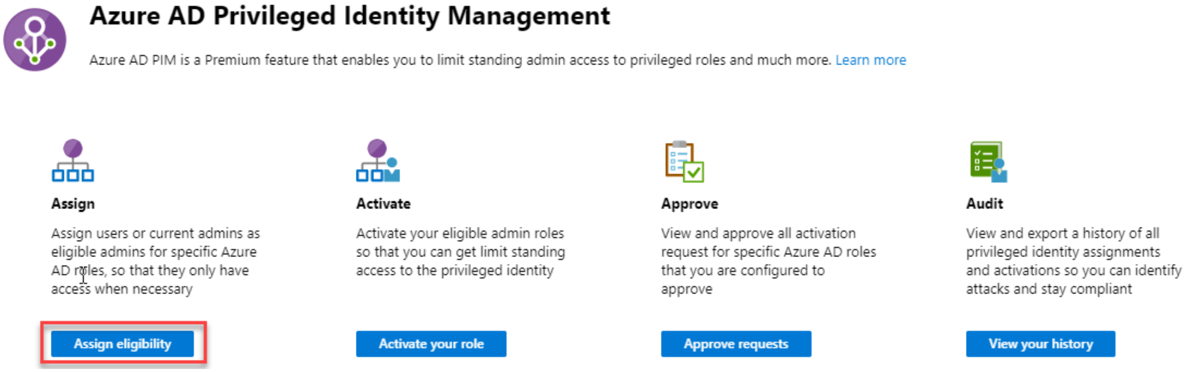
20.0.1 Task 1: Activate a role

When you need to take on an Azure AD directory role, you can request activation by using the **My roles** navigation option in PIM.

1. In the Azure Portal, signed-in as Holly, click **All services** and search for and select `Azure AD Privileged Identity Management`.



2. Click **Azure AD roles**.
3. Click **Quick Start** and click **Assign eligibility**.



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more

Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

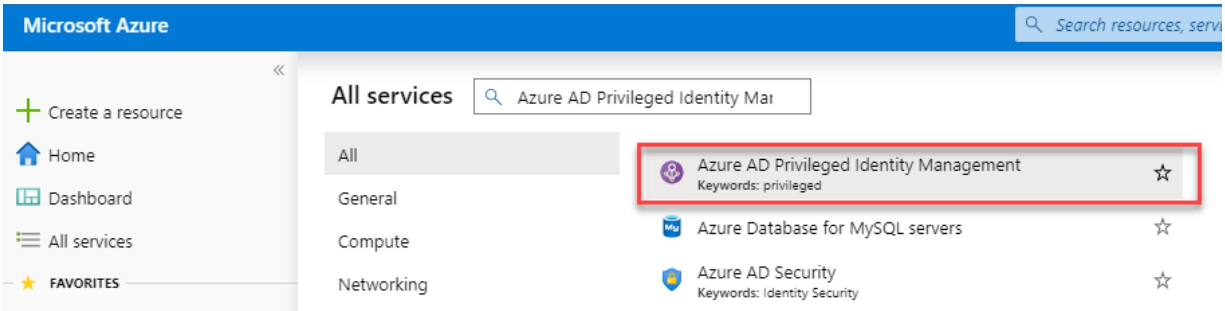
Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve

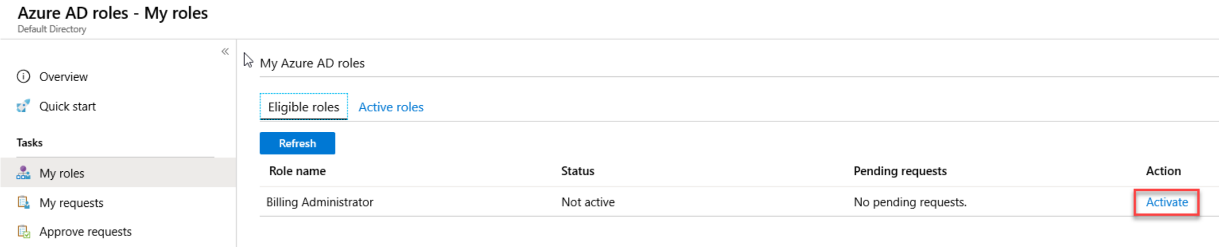
Audit

View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant

4. Click `Billing Administrator` and add Patti Fernandez back into the **Billing Administrators** role.
5. Open an **In Private** browsing session and navigate to `https://portal.azure.com` and login as **Patti** using her UPN. example PattiF@YourTenantHere.onmicrosoft.com with the password given by your lab hoster (hint: the password is likely the same as the MOD Administrator password).
6. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.



7. Click **Azure AD roles**.
8. Click **Quick start** and click **Activate your role**.
9. On the Billing Administrator role, scroll to the right and click **Activate**.

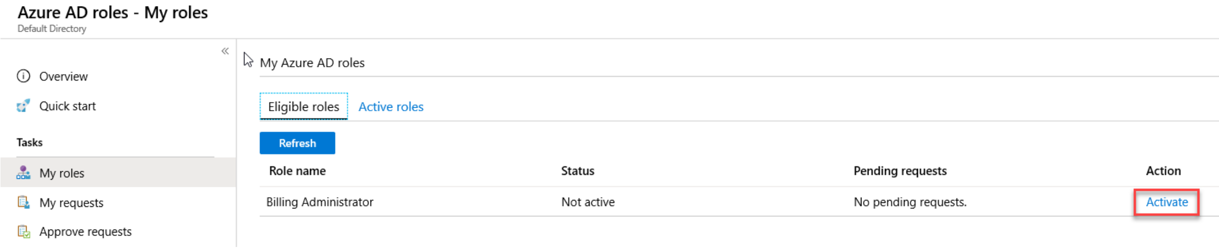


Azure AD roles - My roles

Default Directory

Role name	Status	Pending requests	Action
Billing Administrator	Not active	No pending requests.	Activate

10. Click **Verify your identity before proceeding** if this appears here. You only have to authenticate once per session. Run through the wizard to authenticate Patti.
11. Once returned to the Azure Portal, click **All services** and search for and select `Azure AD Privileged Identity Management`.
12. Select **Azure AD Roles** then click **Activate your role** on the Quick start blade.
13. On the Billing Administrator role, scroll to the right and click **Activate**.

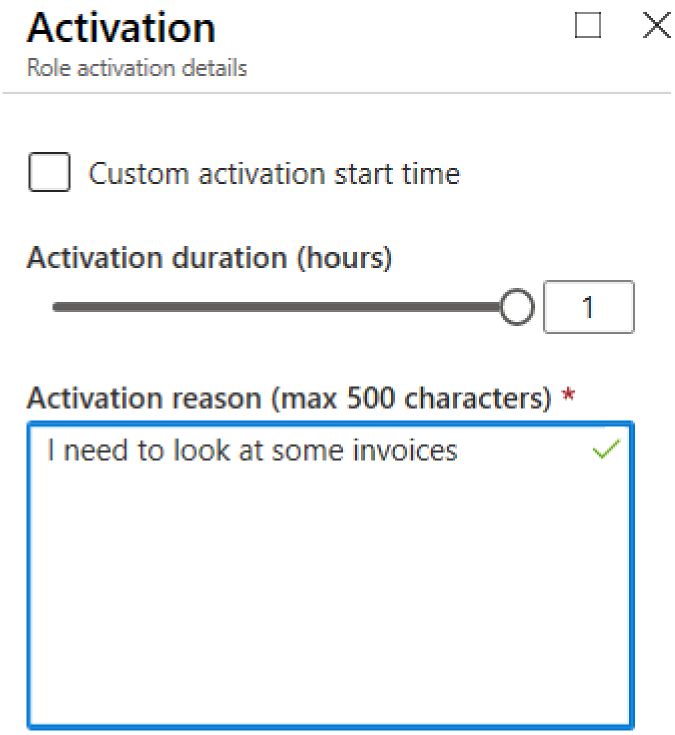


Azure AD roles - My roles

Default Directory

Role name	Status	Pending requests	Action
Billing Administrator	Not active	No pending requests.	Activate

14. Enter an activation reason and click **Activate**



Activation

Role activation details

□ Custom activation start time

Activation duration (hours)

1

Activation reason (max 500 characters) *

I need to look at some invoices ✓

By default, roles do not require approval unless configured explicitly in settings.

If the role does not require approval, it is activated and added to the list of active roles. If you want to use the role right away, follow the steps in the next section.

If the role requires approval to activate, a notification will appear in the upper right corner of your browser informing you the request is pending approval.

20.0.2 Task 2: Use a role immediately after activation

When you activate a role in PIM, it can take up to 10 minutes before you can access the desired administrative portal or perform functions within a specific administrative workload. To force an update of your permissions, use the **Application access** page as described in the following steps.

1. Click **Sign Out**.
2. Log back in as Patti in the inPrivate browsing session.

20.0.3 Task 3: View the status of your requests

You can view the status of your pending requests to activate.

1. Still signed in as **Patti**, in the Azure Portal, click **All services** and search for and select `Azure AD Privileged Identity Management`.
2. Click **Azure AD Roles**.
3. Click **Pending requests** to see a list of your requests.

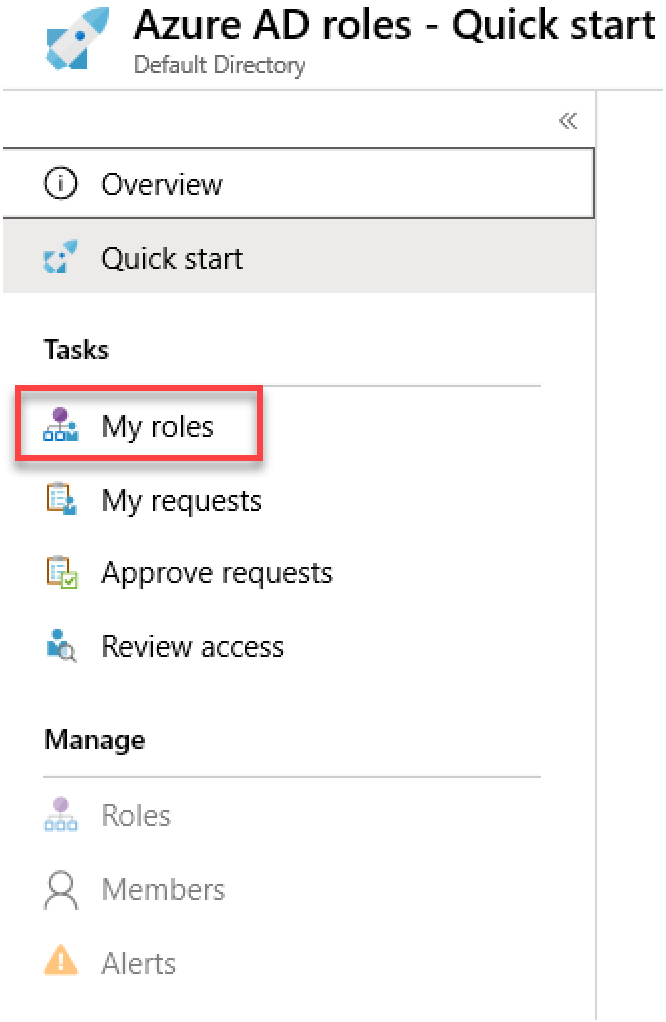
20.0.4 Task 4: Deactivate a role

Once a role has been activated, it automatically deactivates when its time limit (eligible duration) is reached.

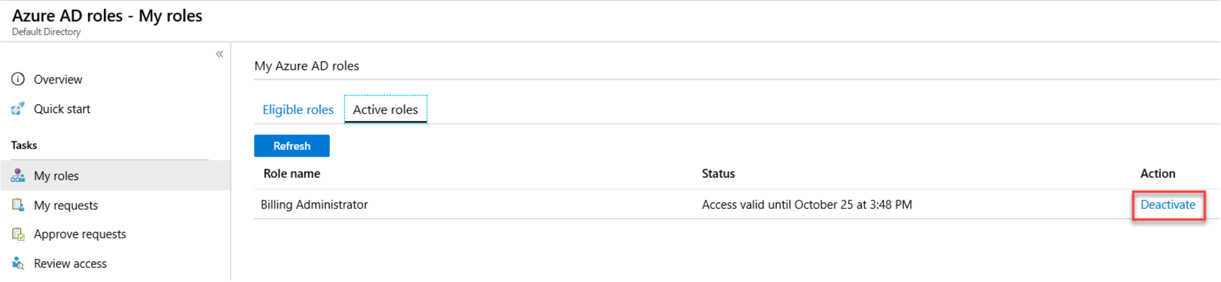
If you complete your administrator tasks early, you can also deactivate a role manually in Azure AD Privileged Identity Management.

1. Still signed in as **Patti**, open Azure AD Privileged Identity Management.
2. Click **Azure AD roles**.

3. Click **My roles**.

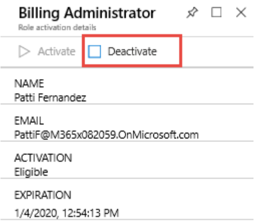


4. Click **Active assignments** to see your list of active roles.
5. Find the role you're done using and then click **Deactivate**.



Role name	Status	Action
Billing Administrator	Access valid until October 25 at 3:48 PM	Deactivate

6. Click **Deactivate** again.



NAME
Patti Fernandez

EMAIL
PattiF@M365x082059.OnMicrosoft.com

ACTIVATION
Eligible

EXPIRATION
1/4/2020, 12:54:13 PM

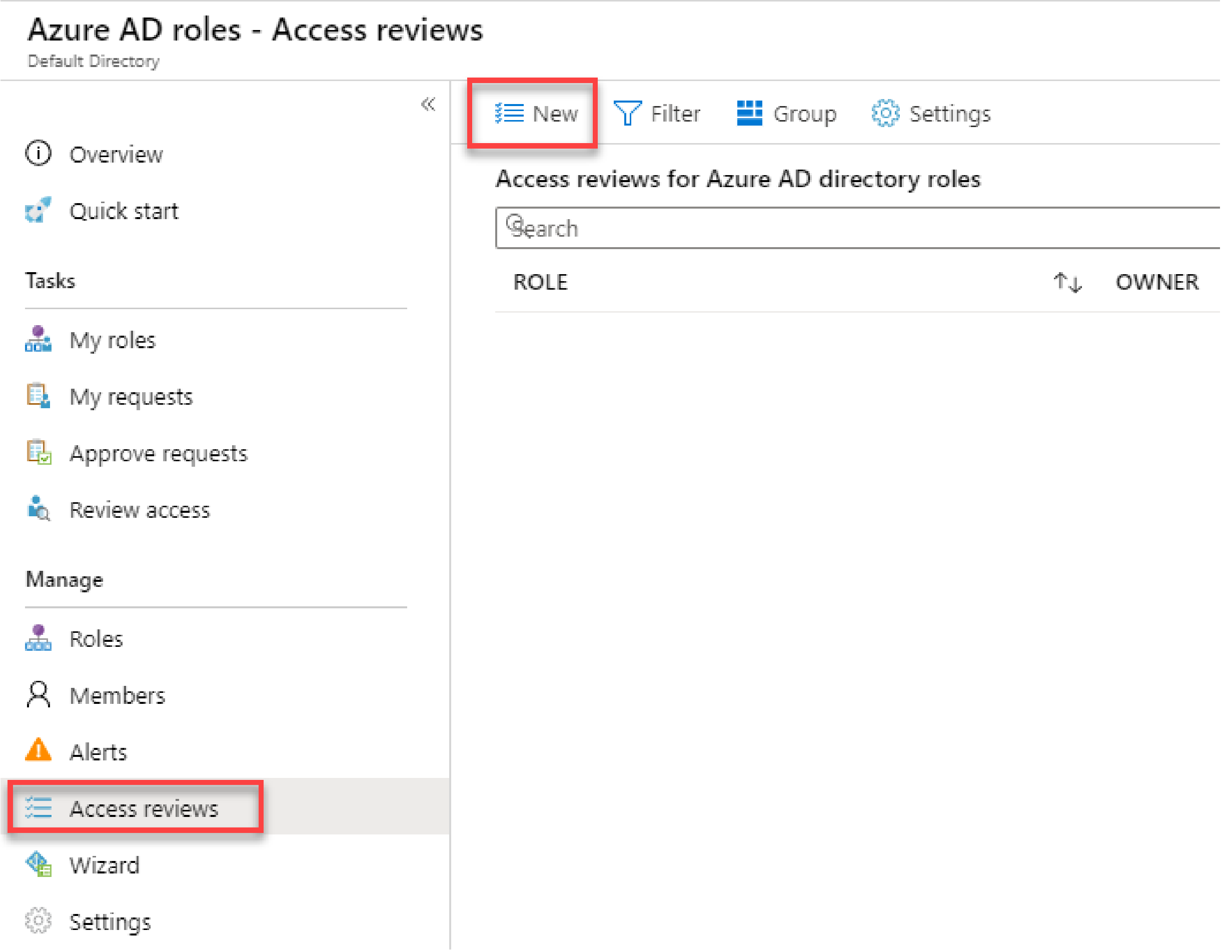
21 Continue to exercise 4

22 Module 3 - Lab 2 - Exercise 4 - Directory Roles (General)

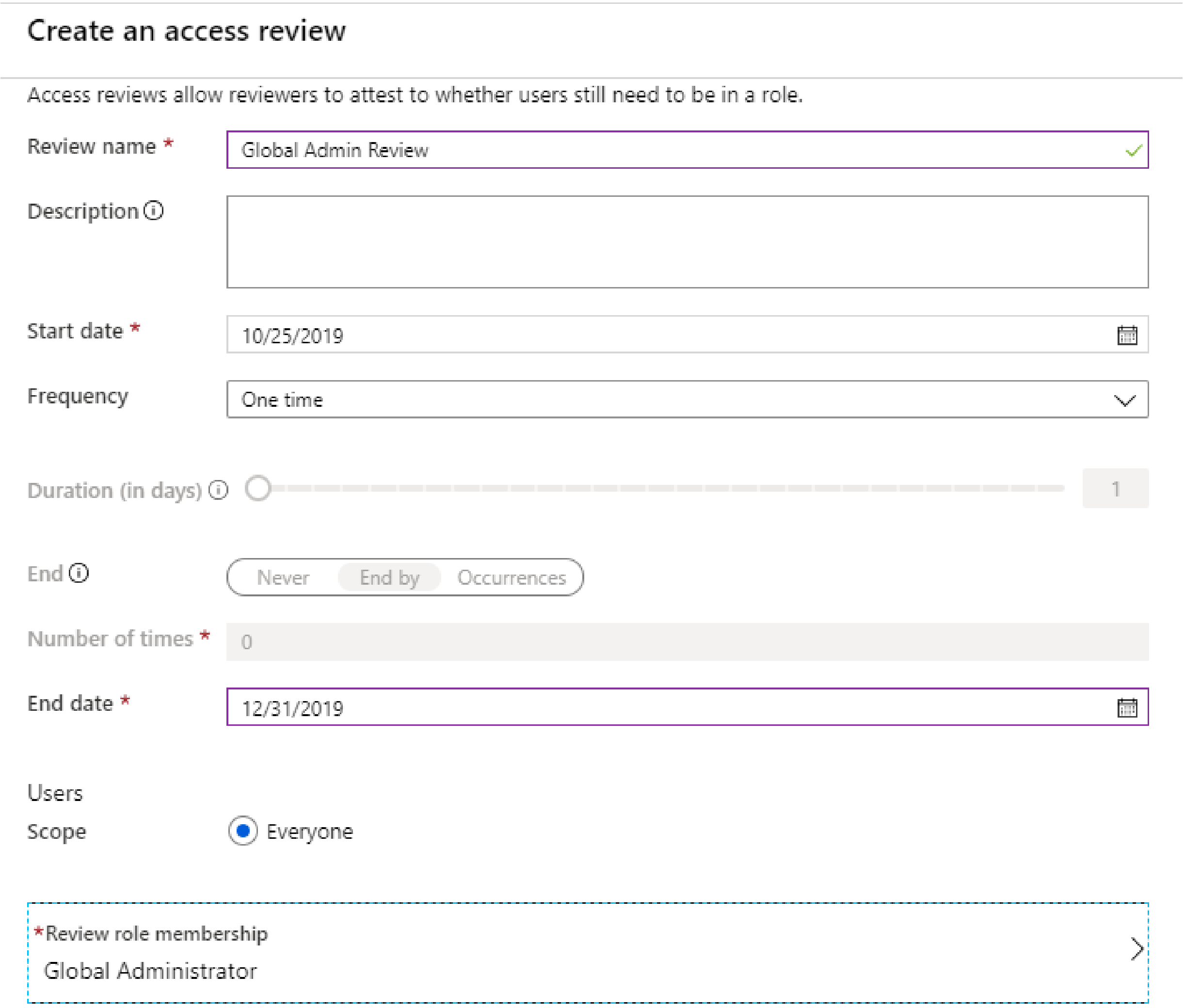
22.0.1 Task 1: Start an access review for Azure AD directory roles in PIM

Role assignments become "stale" when users have privileged access that they don't need anymore. In order to reduce the risk associated with these stale role assignments, privileged role administrators or global administrators should regularly create access reviews to ask admins to review the roles that users have been given. This task covers the steps for starting an access review in Azure AD Privileged Identity Management (PIM).

1. Return back to the browser that is logged in as your Global Admin Account Holly Dickson.
2. From the PIM application main page select **Azure AD Roles** under the **Manage** section select **Access reviews** and Select **New**.



3. Enter the following details and click **Start**:
   - Review name: `Global Admin Review`
   - Start Date: `Today's Date`
   - Frequency: `One time`
   - End Date: `End of next month`
   - Review role membership: `Global Administrator`
   - Reviewers: `Holly Dickson`



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Global Admin Review

Description ⓘ

Start date * 10/25/2019

Frequency One time

Duration (in days) ⓘ 1

End ⓘ Never | End by | Occurrences

Number of times * 0

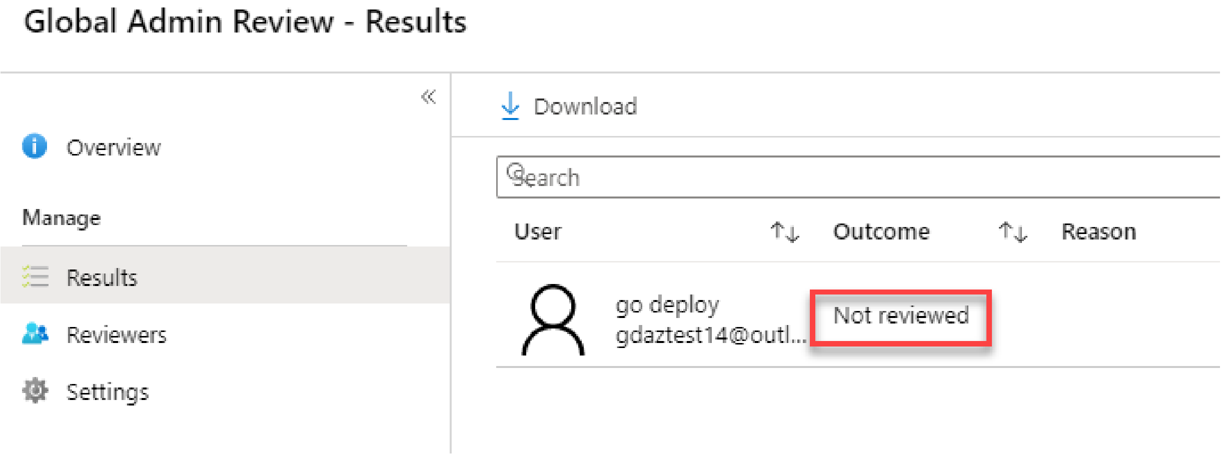
End date * 12/31/2019

Users

Scope ● Everyone

*Review role membership
Global Administrator

4. Once the review has completed and has a status of Active, click on the **Global Admin Review**. You may need to refresh the view in Azure.
5. Select **Results** and see the outcome of **Not reviewed**.



Global Admin Review - Results

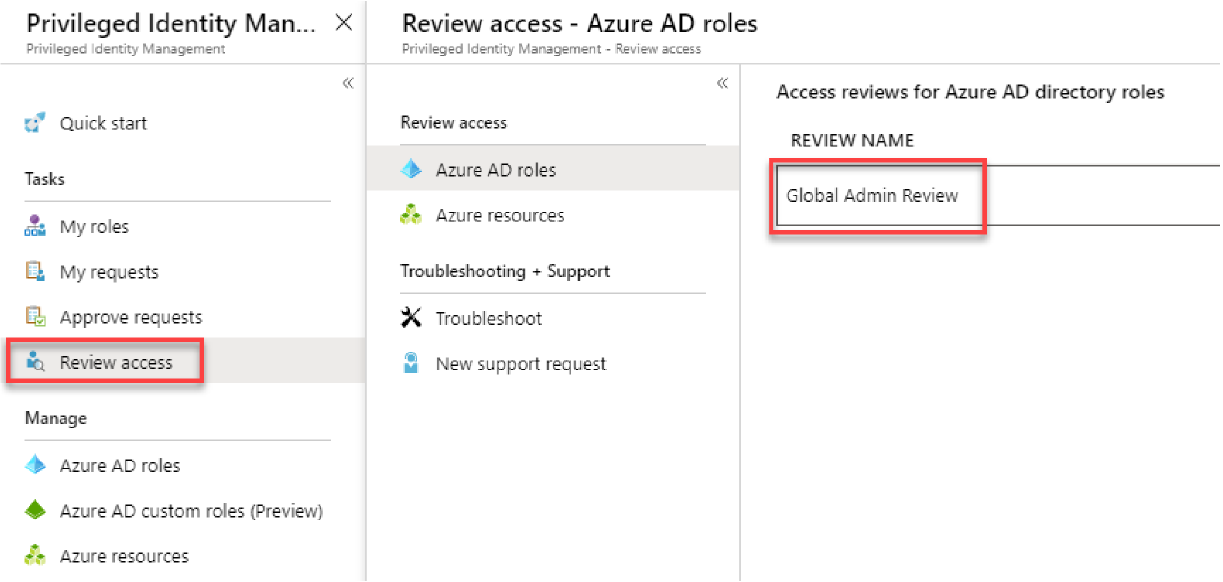
User	Outcome	Reason
go deploy gdaztest14@outl...	Not reviewed	

22.0.2 Task 2: Approve or deny access

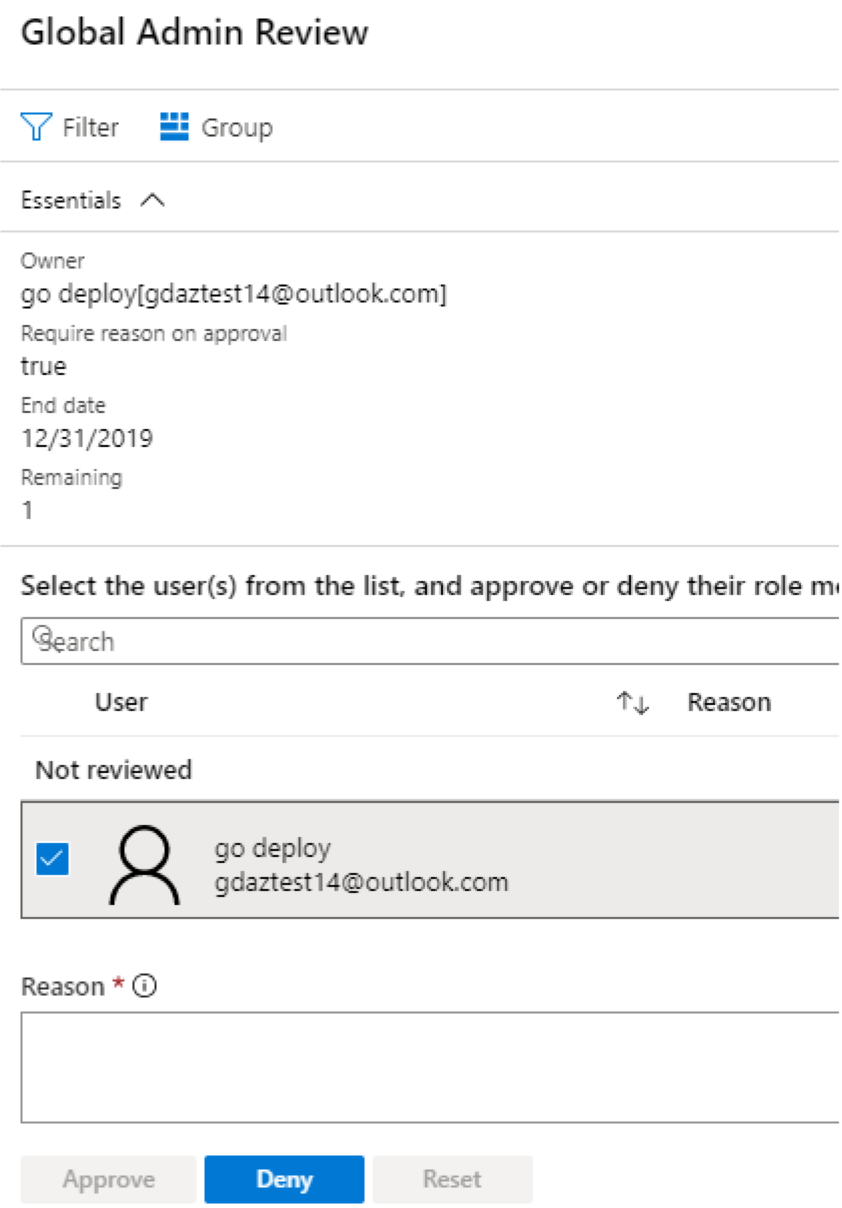
When you approve or deny access, you are just telling the reviewer whether you still use this role or not. Choose Approve if you want to stay in the role, or Deny if you don't need the access anymore. Your status won't change right away, until the reviewer applies the results. Follow these steps to find and complete the access review:

1. In the PIM application, select **Review access**.

2. Select the **Global Admin Review**.


Privileged Identity Man...
Privileged Identity Management
Quick start
Tasks
My roles
My requests
Approve requests
Review access
Manage
Azure AD roles
Azure AD custom roles (Preview)
Azure resources
Review access - Azure AD roles
Privileged Identity Management - Review access
Review access
Azure AD roles
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Access reviews for Azure AD directory roles
REVIEW NAME
Global Admin Review

3. Unless you created the review, you appear as the only user in the review. Select the check box next to Holly Dickson and click **view**.


Global Admin Review

Owner
go deploy[gdaztest14@outlook.com]
Require reason on approval
true
End date
12/31/2019
Remaining
1

Select the user(s) from the list, and approve or deny their role m

☑ go deploy
gdaztest14@outlook.com

Reason *

4. Close the **Review Azure AD roles** blade.

22.0.3 Task 3: Complete an access review for Azure AD directory roles in PIM

Privileged role administrators can review privileged access once an access review has been started. Azure AD Privileged Identity Management (PIM) will automatically send an email prompting users to review their access. If a user did not get an email, you can send them the instructions in how to perform an access review.

After the access review period is over, or all the users have finished their self-review, follow the steps in this task to manage the review and see the results.

1. Go to the **Azure portal** and select the `Azure AD Privileged Identity Management`.
2. Select **Azure AD Roles**.
3. Select the **Access reviews**.
4. Select the Global Admin Review.
5. Choose one of the available options for completing the review:
   - **Stop** - All access reviews have an end date, but you can use the Stop button to finish it early. If any users haven't been reviewed by this time, they won't be able to after you stop the review. You cannot restart a review after it's been stopped.

- **Apply** - After an access review is completed, either because you reached the end date or stopped it manually, the Apply button implements the outcome of the review. If a user's access was denied in the review, this is the step that will remove their role assignment.
- **Delete** - If you are not interested in the review any further, delete it. The Delete button removes the review from the Privileged Identity Management service.

22.0.4 Task 4: Configure security alerts for Azure AD directory roles in PIM

You can customize some of the security alerts in PIM to work with your environment and security goals. Follow these steps to open the security alert settings:

1. Open `Azure AD Privileged Identity Management`.
2. Click **Azure AD roles**.
3. Click **Alerts** and then **Setting**.
4. Click an alert name to configure the setting for that alert.

23 continue to exercise 5

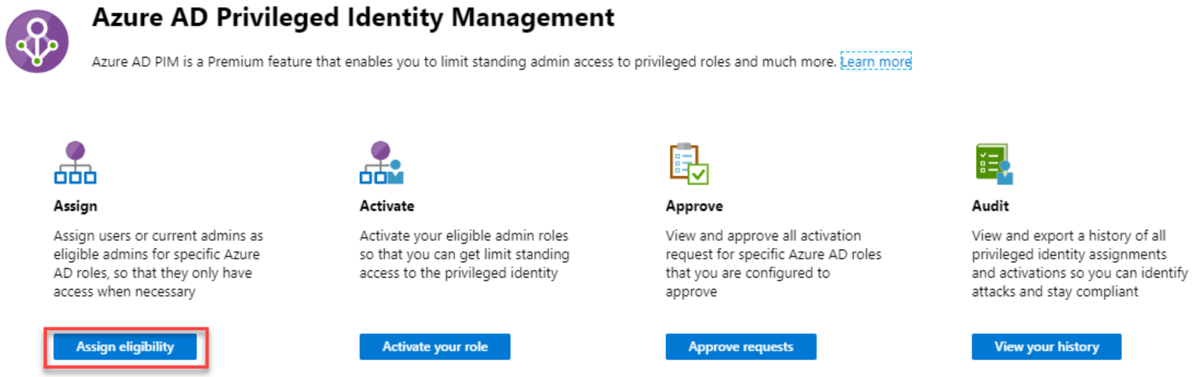
24 Module 3 - Lab 2 - Exercise 5 - PIM resource workflows

24.0.1 Task 1: Configure the Global Administrator role to require approval.

1. You should still be logged in as Holly from the previous exercise. Open `Azure AD Privileged Identity Management`.
2. Click **Azure AD roles**.
3. Click **Settings**
4. Select `Global Administrator`.
5. Click **Edit**, scroll down and mark **Require Approval to activate**.
6. Click **Select approver(s)** and assign Holly Dickson as the approver and click **Select**. Then click **Update**.

24.0.2 Task 2: Enable Patti for Global Administrator privileges.

1. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click the **Quick Start** and select **Assign eligibility**.



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more

Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

Approve

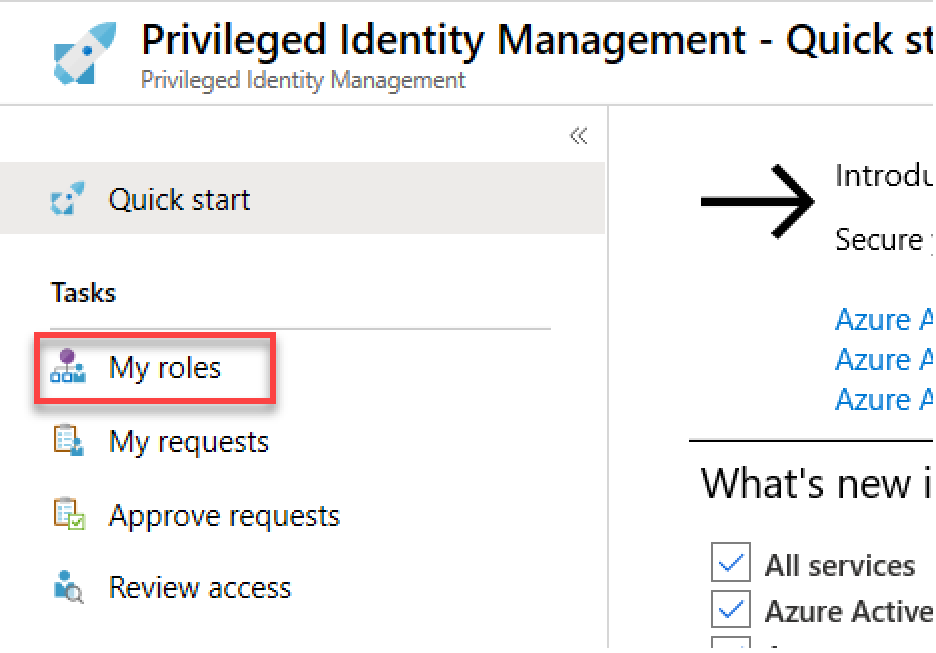
View and approve all activation request for specific Azure AD roles that you are configured to approve

Audit

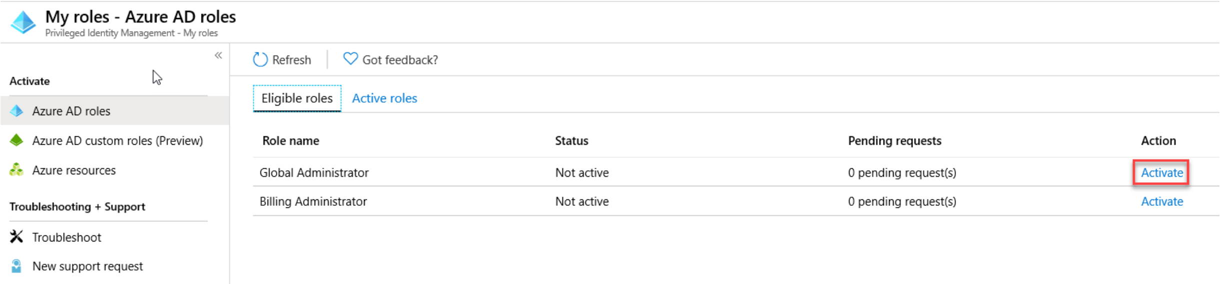
View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant

4. Select **Global Administrator**.
5. Select + **Add assignments** and select **Patti Fernandez**. Click **Select**.
6. Click **Next** and then click **Assign**.
7. Open an in Private Browsing session and login to `https://portal.azure.com` as Patti Fernandez. You might still have this browser open from earlier exercise.

8. Open **Azure AD Privileged Identity Management**.
9. Select **My Roles**.



10. **Activate** the Global Administrator Role.


My roles - Azure AD roles
Privileged Identity Management - My roles
Activate
Azure AD roles
Azure AD custom roles (Preview)
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Got feedback?
Eligible roles
Active roles

Role name	Status	Pending requests	Action
Global Administrator	Not active	0 pending request(s)	Activate
Billing Administrator	Not active	0 pending request(s)	Activate

11. Verify Patti's identity using the wizard if necessary.
12. Return back to **My Roles** in **Azure AD Privileged Identity Management**.
13. Click **Activate** near the Global Administrator Role.
14. Enter a reason for the activation **I need to carry out some administrative tasks** and click **Activate**.

Eventually you should see a notice that your request is ”pending approval”.

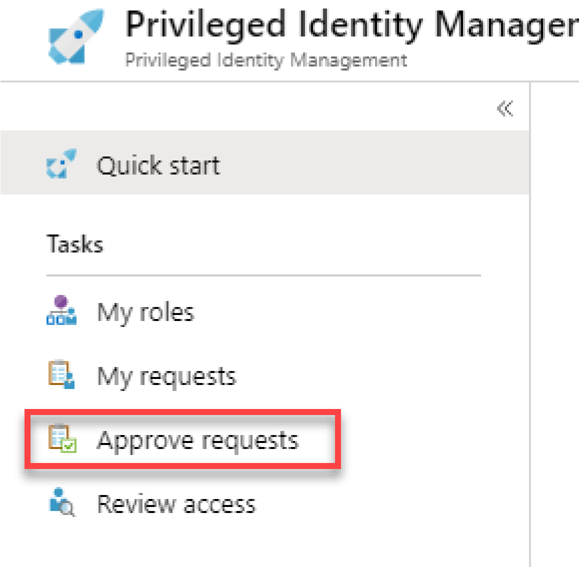
24.0.3 Task 3: Approve or deny requests for Azure resource roles in PIM

With Azure AD Privileged Identity Management (PIM), you can configure roles to require approval for activation, and choose one or multiple users or groups as delegated approvers. Follow the steps in this article to approve or deny requests for Azure resource roles.

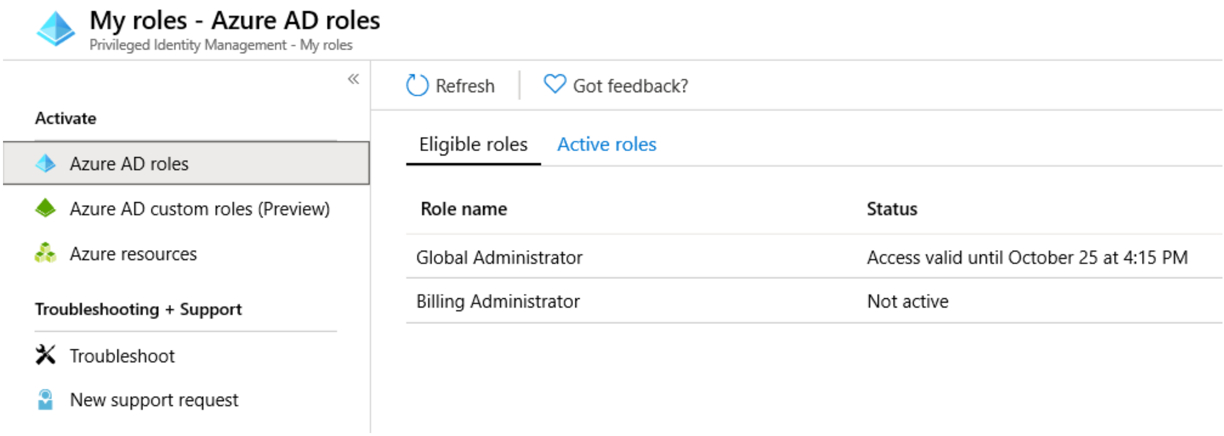
View pending requests

As a delegated approver, you will receive an email notification when an Azure resource role request is pending your approval. You can view these pending requests in PIM.

1. Switch back to the browser you are signed in with your Global Administrative account Holly Dickson.
2. Open **Azure AD Privileged Identity Management**.
3. Click **Approve requests**.



4. Select the request from Patti and click **Approve**.
5. Enter a reason **Granted for this task** and click **Confirm**.
6. A notification appears that Patti is approved.
7. Switch back to the In Private Browsing session where Patti is signed in and click **My Roles** and then select **Active assignments** note the status is now activated for Global Administrator.


My roles - Azure AD roles
Privileged Identity Management - My roles
Activate
Azure AD roles
Azure AD custom roles (Preview)
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Got feedback?
Eligible roles
Active roles

Role name	Status
Global Administrator	Access valid until October 25 at 4:15 PM
Billing Administrator	Not active

25 continue to exercise 6

26 Module 3 - Lab 2 - Exercise 6 - View audit history for Azure AD roles in PIM

You can use the Azure Active Directory (Azure AD) Privileged Identity Management (PIM) audit history to see all the role assignments and activations within the past 30 days for all privileged roles. If you want to see the full audit history of activity in your directory, including administrator, end user, and synchronization activity, you can use the Azure Active Directory security and activity reports.

26.0.1 Task 1: View audit history

Follow these steps to view the audit history for Azure AD roles.

1. As Holly Dickson open `Azure AD Privileged Identity Management`.
2. Click **Azure AD roles**.
3. Click **View your history** button from the Quick start area.

Depending on your audit history, a column chart is displayed along with the total activations, max activations per day, and average activations per day.

At the bottom of the page, a table is displayed with information about each action in the available audit history. The columns have the following meanings:

4. To change the variable select the different options and click **Apply**.
5. If you desire you can export the data results by clicking the **Export** button. This will export the results to a *.CSV file.

Results: You have now completed this lab.

27 End lab

28 Module 4: Lab 1 - Exercise 1 - Improve your secure score in Microsoft 365 Security Center

You are the Global Admin Holly Dickson, and you are signed into Microsoft 365.

With so many services offering security benefits, it is often difficult for Holly to know what steps she should take first to secure her organizations deployment. The Microsoft secure score reviews her security recommendations and prioritizes them, so she can know which recommendations to prioritize. In this exercise Holly is going to view her organization's Microsoft secure score and use the portal to take a recommended action to improve the score.

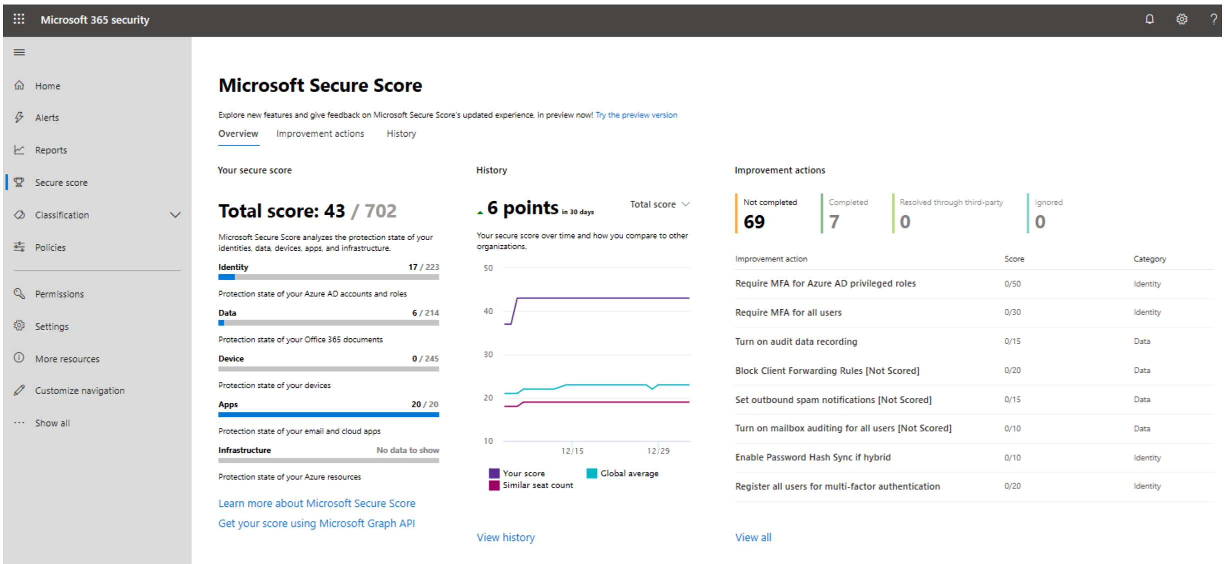
Secure score calculation

Security Center mimics the work of a security analyst, reviewing your security recommendations, and applying advanced algorithms to determine how crucial each recommendation is.

Microsoft Security center constantly reviews active recommendations and calculates your secure score based on them, the score of a recommendation is derived from its severity and security best practices that will affect your workload security the most.

28.0.1 Task 1: View the secure score in the Microsoft 365 Security Portal.

1. Login to **LON-CL1** virtual machine as Administrator with the password: `Pa55w.rd`. Go to the Microsoft 365 security dashboard `https://security.microsoft.com` and login with Holly's global admin credentials, select **Microsoft Secure score** on the dashboard.
2. At the top you can see Secure score highlights:
   - The **Secure Score** represents the score per policies, per selected subscription
   - Secure score by category shows you which resources need the most attention



Microsoft Secure Score

Explore new features and give feedback on Microsoft Secure Score's updated experience, in preview now! Try the preview version

Overview Improvement actions History

Your secure score

Total score: 43 / 702

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

Identity 17 / 223
Protection state of your Azure AD accounts and roles

Data 6 / 214
Protection state of your Office 365 documents

Device 0 / 245
Protection state of your devices

Apps 20 / 20
Protection state of your email and cloud apps

Infrastructure No data to show
Protection state of your Azure resources

Learn more about Microsoft Secure Score
Get your score using Microsoft Graph API

History

6 points in 30 days Total score

Your secure score over time and how you compare to other organizations.

View history

Improvement actions

Not completed 69 | Completed 7 | Resolved through third-party 0 | Ignored 0

Improvement action	Score	Category
Require MFA for Azure AD privileged roles	0/50	Identity
Require MFA for all users	0/30	Identity
Turn on audit data recording	0/15	Data
Block Client Forwarding Rules [Not Scored]	0/20	Data
Set outbound spam notifications [Not Scored]	0/15	Data
Turn on mailbox auditing for all users [Not Scored]	0/10	Data
Enable Password Hash Sync if hybrid	0/10	Identity
Register all users for multi-factor authentication	0/20	Identity

View all

Note: The sum of the secure score of each subscription does not equal the overall secure score. The secure score is a calculation based on the ratio between your healthy resources and your total resources per recommendation, not a sum of secure scores across your subscriptions.

3. Select **Improvement actions** to see the actions you can take to improve the secure score for that subscription.
4. In the list of actions, you can see that for each action there is a column that represents the **Points achieved**. This number represents how many of the possible points you have achieved by taking the action. For example, in the screen below, if you **Require MFA for administrative roles**, you can score up to ten points.

28.0.2 Task 2: View the Microsoft Secure Score History.

In addition, you can view the history of your secure score, click the **History** option.

You can customize the day range for the view and focus on specific secure score categories. This will give you a sense of how your security posture has changed over time.

The Secure Score History view also lists specific actions you have taken and the impact it has had on your score.

28.0.3 Task 3: Improve your Secure Score

1. Click the **Improvement actions** tab and select **Enable self-service password reset**. More information about this security action appears. Notice it includes specific instructions to take this action.
2. Click the **Manage** button. A new browser tab should open directly to the **Password reset - Properties** blade in Azure portal.
3. Under **Self service password reset enabled** click All.
4. Click **Save** if it was not already set to All from an earlier lab.
5. In the Manage area click **Registration**.
6. Make sure ”Require users to register when signing in?” is marked **Yes**.
7. Change the Number of days before users are asked to re-confirm their authentication information to `90`.
8. Click **Save**.
9. Return the browser tab with Microsoft Secure Score.
10. In the Enable sef-service password reset pane in the Notes enter the following **Enabled Self-Service password reset for all users on <enter today’s date>** and click **Save and close**.

Note: Score updates may take 24 hours to appear in your Microsoft Secure Score. Also, partial score may be given depending on the action. For example, this tenant includes 10 licensed users, if just two of the users were enabled for Self service password reset 1/5 points would be awarded for this action.

Return to Microsoft Secure Score in 24 hours to view the change to your score and revisit History tab.

Results: In this lab, you learned how to improve your secure score in the Microsoft Security Center.

29 End of Lab

30 Module 5 - Lab 1 - Exercise 1 - Implement ATP Policies

You have a Global Admin account set up for Holly Dickson, and you’re signed into Microsoft 365 as Holly. In this phase of your pilot project for Adatum, you want to edit an existing ATP Safe Links policy, and then create a Safe Attachments policy and turn on Advanced Threat Protection for SharePoint, OneDrive, and Microsoft Teams. You will also validate both policies to ensure they work properly.

30.0.1 Task 1 – Create a Safe Links Policy

In this task, you will add the URL **http://tailspintoys.com** to the company-wide list of blocked URLs, and you will create an ATP safe links recipient policy that applies to all users in your tenant.

1. You should still be logged into your Client 1 VM (**LON-CL1**) as the **LON-CL1\Admin** account, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. You should still be in the Microsoft 365 Security and Compliance center. If not, in your browser, enter `https://protection.office.com`
3. In the **Security & Compliance center**, in the left navigation pane, select **Threat Management** and then select **Policy**.
4. In the **Policy** window, scroll to the right (if necessary) and select the **Safe Links** tile.
5. In the **Safe Links** window, click **Global Settings**.
6. In the **Global settings for users included in active Safe Links policies** window, under the **Block the following URLs** section, you can enter any URLs that you want to have blocked. For this test lab, in the **Enter a valid URL** field, enter `http://tailspintoys.com` to add it to the policy.
7. Select **Save**. Click **OK**.
8. Select the **+ Create** to add a new recipient policy.
9. On the **Name your policy** pane, enter `All company users` in the **Name** field.
10. On the **Settings** pane, select the following options:
    - Under **Select the action for unknown potentially malicious URLs in messages**: Select **On – URLs will be rewritten and checked against a list of known malicious links when user clicks on the link**.
    - Also select **On** for unknown or potentially malicious URLs within Microsoft Teams.
    - Select the check box next to **Apply real-time URL scanning for suspicious links and links that point to files**.
    - Select the check box next to **Apply safe links to email messages sent within the organization**.
11. On the **Notification** pane, leave the default notification text selected.
12. On the **Applied To** section, click the **+ Add a condition** drop down arrow, and then in the drop-down menu, select **The recipient domain is** and click "**Choose**".
    - In the pop-up window that appears, click "**+ Add**", select the available domain **M365xZZZZZZ.onmicrosoft.co** Click **Add** and then select **Done** and **Next**
13. On the **Review your settings** pane, select **Finish** to create the policy.
14. Leave the Office 365 Security & Compliance tab open for use in a later task.

30.0.2 Task 2 – Validate the Safe Links Policy

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

1. You should still be logged into your Client 1 VM (**LON-CL1**) as the **LON-CL1\Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, select the **Microsoft Office Home** (or go to `https://office.com`) tab and then select **Outlook.**
3. If you receive a **We updated Outlook** message, select **Not Now**, or if you see a **Welcome** message, then close it.
4. In **Outlook on the web**, select **New Message** in the upper left part of the screen.
5. In the right pane, enter the following email information:
    - To: You will be sending an email to the MOD Administrator, so enter **mod** in the **To** field and then select the **MOD Administrator** email address from the drop-down list.
    - Add a subject: `Free stuff from Microsoft`
    - Add a message: `Please click on me for free toys from Microsoft.`
6. Select the text that you added in the body of the message.

7. At the bottom of the detail pane, below the body of the message, is a taskbar. On the taskbar, select the **Insert hyperlink** icon to display the Insert link window.
8. In the **Insert link** window, the text that you highlighted in the body of the message should be displayed in the **Display as** field. In the **Web address (URL)** field, enter the following URL: `http://tailspintoys.com/aboutus/freetoys`.
9. Select **OK**.
10. In the body of the email, the message should still be selected. Click anywhere in the body of the message to remove the highlighting. The color of the text should now be blue and it should be underlined, indicating that this message is hyperlinked to a URL.
11. Select **Send** in the menu bar that appears above the message (or the **Send** button at the bottom of the page).
12. You now want to open the MOD Administrator's Inbox in Outlook and validate whether the ATP policy you created in the prior task worked on the email that you just sent from Holly. To do this, you must switch the Client 2 VM (LON-CL2).
13. Log into the VM as the **Admin** account by entering **Ps55w.rd** in the **Password** field if necessary.
14. Select the **Microsoft Edge** icon in the taskbar, maximize the window and then enter the following URL in the address bar: `https://outlook.office365.com`
15. Since you want to sign in as the MOD Administrator, in the **Sign-in** window, enter **admin@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your tenant ID provided by your lab hosting provider) and then select **Next**.
16. In the **Enter password** window, enter the password provided by your lab hosting provider and select **Sign in**. If you are requested to provice self-service password information click **cancel**.
17. Close the **Let Microsoft Edge save and fill your password for this site next time?** banner by selecting **Never**.
18. On the **Stay signed in?** dialog box, select the **Don't show this again** check box and then select **Yes.**
19. Close the **Welcome** window that appears.
20. In the MOD Administrator's **Inbox**, open the email that was sent by Holly.
21. When you hover over the blue link that appears in the body of the email, you can see a long URL in the bottom of the browser window; this URL starts with `https://nam03.safelinks.protection.outlook.com`.

    When you select the hyperlink to open it, a new tab in **Edge** opens that displays the following warning message: **Opening this website might not be safe.** This message indicates that your ATP Safe Links policy is working correctly and access to the URL is blocked with ATP Safe Links.
22. Leave the Client 2 VM open and leave Outlook open to the MOD Administrator's Inbox for later.

30.0.3 Task 3 – Create a Safe Attachment policy and turn on ATP for SharePoint, OneDrive, and Microsoft Teams

In this task, you will, and you'll create an ATP Safe Attachments policy that will test email attachments for malware that are sent to recipients within the M365xZZZZZZ.on microsoft.com domain. You will configure the policy so that if an attachment is blocked, it will be removed from the email that is sent to the recipient, and a copy of the email will be redirected to Joni Sherman for additional review.

1. Switch back to your Client 1 VM (**LON-CL1**). You should still be logged into your Client 1 VM as the **LON-CL1\Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Edge** browser, select the **Office 365 Security & Compliance** tab.
3. In the **Office 365 Security & Compliance center**, in the left navigation pane under **Threat Management**, select **Policy**.
4. In the **Policy** window, select the **Safe Attachments** tile.
5. On the **Safe attachments** window, at the top of the page under **Global Settings** in the **Protect files in SharePoint, OneDrive, and Microsoft Teams** section, select the **Turn on Defender for Office 365 for SharePoint, OneDrive and Microsoft Teams** switch. Select **Save**.

6. Select the + **Create** on the menu bar to add a new safe attachments policy.
7. In the new safe attachments policy window, enter `AttachmentPolicy1` in the **Name** field then select **Next**
8. Under the **Safe attachments unknown malware response** section, select **Dynamic Delivery** (this option will still send the email but will hold the attachment until it has been scanned and marked acceptable).
9. Under the **Redirect attachment on detection** section, select **OK**.
10. In the **Send the attachment to the following email address** field, enter **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
11. Scroll down in the window and under the **Applied To** section, under **If** (the first condition), select the drop-down arrow and select **The recipient domain is...**
12. In the **NAME** dialog box, select the **M365xZZZZZZ.onmicrosoft** domain (where ZZZZZZ is your tenant ID provided by your lab hosting provider), select **add->**, and then select **Done** then click **Next**.
13. On the **Review Settings** window, note the two messages displayed regarding the **Dynamic Delivery** and **Enable redirect** options that were selected. select **Finish**.
14. It may take a minute or so to update the organization settings. In the **Update complete** window, select **OK**.

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

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

31 End of Lab

32 Module 6 - Lab 1 - Exercise 1 - Conduct a Spear phishing attack

Holly Dickson is concerned that some users in her organization may require education about phishing attacks. In this lab you will use the Microsoft 365 Attack simulator to determine your users' susceptibility to phishing attacks.

32.0.1 Task 1: Enable Mulit-factor authentication for Holly Dickson

1. On LON-CL1, Go to the Office 365 Security & Compliance center `https://protection.office.com` and login as **Holly Dickson**.
2. Click **Threat management**, and then click **Attack simulator**.
3. Notice the warning that you must enable multi-factor authentication (MFA). You are about to do a simulated attack and the system wants to confirm your credentials. This is a requirement of the attack simulator. Let's enable MFA for Holly Dickson. Go to your browser tab with the Microsoft 365 admin center or open a new browser tab to `https://admin.microsoft.com`.

   Note: You may not get this warning if you enabled MFA for Holly in an earlier lab and are using the same tenant. If this is the case you may skip ahead to the next task.
4. On the left select **Users** and then select **Active users**.
5. On the Active users screen click **Multi-factor authentication**.
6. In the multi-factor authentication screen View **Global Administrators** then select **Holly Dickson** and select **Enable** under quick steps.

7. In the About enabling multi-factor auth screen select **enable**. in the About enabling multi-factor auth screen select **enable multi-factor auth** button.

8. In the Updates successful screen click **Close**.

9. Close the browser session. Open a new browser and open the Office 365 Security & Compliance portal and login again as Holly Dickson. Now you should be asked for multi-factor credentials as part of the login process.

```
**Note:** it may take several minutes for this MFA setting to propagate your tenant.  If the **Launch A
```

32.0.2 Task 2: Configure and launch a Spear Phishing attack

1. Go to Microsoft 365 security center - Attack simulation training and login as **Holly Dickson**.

2. Click the **Simulations** tab. Select **+ Launch a Simulation**.

3. On the **Select Technique** screen. Ensure that **Credential Harvest** is selected. Click **Next**.

4. Name the simulation `Spear Simulation` and select **Next**.

5. On the **Select Payload** screen, select a desired payload from the list of provided payloads. Click **Next**.

6. In the **Target Users** screen, do the following:

    1. Ensure **Include only specific users and groups** is selected.
    2. Click **Add Users**.
    3. On the **Add Users** screen, type **Patti Fernandez** in the search box and hit Enter.
    4. Select the user from the search results list.
    5. Click **Add 1 User** at the bottom.
    6. Click **Next**.

7. Leave the default settings on the **Assign training** screen. Click **Next**.

8. On the **Launch Details** page, ensure that **Launch this simulation as soon as I'm done** is selected. Click **Next**.

9. On the **Review Simulation** screen, click **Submit**.

32.0.3 Task 3: Confirm target received phishing email attack

2. Open a new browser window in InPrivate or incognito mode and browse to `https://office.com`.

3. Log in as the user Patti Fernandez **PattiF@M365xZZZZZZ.onmicrosoft.com** where ZZZZZZ is your specific Office 365 tenant. Patti's password is likely the same as the MOD administrator's password provided by your lab hosting providor.

4. Click the Outlook icon to open Microsoft Outlook for Patti. You should see a spear phishing email that includes the details you just entered in the previous task.

32.0.4 Task 4: Review the results

3. In your browser session where you are logged in as Holly Dickson go back to the Attack simulation training. Click the **Simulations** tab.

4. In the Spear Phishing (Credentials Harvest) area click **Attack Details**. Notice in the Attack History area it lists how many users were compromised by the attack.

5. In the Attack History area if you select the Export button it will export a list of users who fell victim to the simulated spear-phishing attack.

    Note: Since you can run multiple spear phishing simulation campaigns simultaneously you could create different simulations for different users and groups. These different simulations might have enticements that are more appropriate for different users.

33 Continue to exercise 2.

34 Module 8 - Lab 1 - Exercise 1 - Enable device management

You are Holly Dickson the security administrator for Adatum Corporation, and you have Microsoft 365 deployed in a virtualized lab environment. In this lab, you will manage user devices using Intune.

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

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

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

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account and into Microsoft 365 as Holly Dickson (**holly@M365xZZZZZZ.onmicrosoft.com**) with a password of **Pa55w.rd**.
2. In **Microsoft Edge**, you should still have a tab open to the **Microsoft 365 admin center**; if so, select that tab now. If not, enter **https://portal.office.com**, sign in as **Holly**, and in the **Microsoft Office Home** page, select **Admin**.
3. In the **Microsoft 365 admin center**, select **Billing** in the left navigation pane, and then under it, select **Licenses**.
4. On the **Licenses** page, select **Enterprise Mobility + Security E5.**
5. In the **Enterprise Mobility + Security E5** page, under the list of users, verify that your pilot team members – **Alex Wilber**, **Joni Sherman**, **Lynne Robbins**, and the **MOD Administrator** – were each assigned a license.

   Note: These user accounts were created as part of your Office 365 tenant, and during that process, they were each assigned an Office 365 E5 license and an Enterprise Mobility + Security E5 license.
6. The one user who was not assigned an Enterprise Mobility + Security E5 license is your Global Administrator, Holly Dickson. When you created Holly's user account in an earlier lab, you may have been instructed at that time to only assign her an Office 365 E5 license. You will now assign her an Enterprise Mobility + Security E5 license. If Holly already has an Enterprise Mobility + Security E5 license you can skip to the next task.

   To assign Holly a license, select **+Assign licenses**.
7. On the **Assign licenses to users** page, select the **Enter a name or email address** field, and in the list of users that appears, select **Holly Dickson**.
8. Select **Assign**.
9. Close the **You assigned a license to Holly Dickson** window.
10. Leave your Client 1 VM open for the remainder of this lab.

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

35 Proceed to Exercise 2

36 Module 8 - Lab 1 - Exercise 2 - Configure Azure AD for Intune

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

36.0.1 Task 1: Integrate Azure AD with Intune

1. You should still be logged into your Client 1 VM (LON-CL1) as the **Admin** and in Microsoft 365 as **Holly Dickson**.
2. In the **Azure portal** , in the **All services** box, search for and select **Azure Active Directory**.
3. On the **Adatum Corporation - Overview** window, in the left pane under **Manage** select **Mobility (MDM and MAM),** and then in the details pane on the right, select **Microsoft Intune**.

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

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

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

36.0.2 Task 2: Configure Azure AD join

1. In the **Azure portal** , in the left navigation pane, select **Azure Active Directory.**
2. In the **Adatum Corporation** – **Overview** window, in the left section under **Manage**, select **Devices**.
3. In the **Devices** – **All devices** window, in the details pane on the right, verify that no devices are listed. This is because no device has yet to be joined to Azure Active Directory.
4. In the **Devices** – **All devices** window, in the left pane, select **Device settings**.
5. In the details pane that appears on the right, the property **Users may join devices to Azure AD** is currently set to **All**. This means that all Azure AD users can join their devices to Azure Active Directory. Click **Selected** instead.
6. Below this field, in the **Selected** section click **No member selected**.
7. In the **Members allowed to join devices** window, select **+Add**
8. In the **Add members** pane on the right, select **Alex Wilber** , select **Select** at the bottom of the screen, and then select **Ok**.
9. Back in the **Device settings** detail pane on the right, scroll down and verify that **Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication** is set to **No**. The **Maximum number of devices per user** property is currently set to **50.** Select **10** from the drop down box.
10. In the menu bar at the top of the detail pane, select **Save**.
11. Leave the Azure portal open for the next task.

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

36.0.3 Task 3: Create dynamic Azure AD device group

1. In the **Azure portal** , in the left navigation pane, select **Azure Active Directory.**
2. In the **Adatum Corporation** – **Overview** window, in the left section under **Manage,** select **Groups**.
3. In the **Groups** – **All groups** window, in the details pane on the right, select **+New group** on the menu bar.
4. In the **New Group** window, enter the following information:

   - Group type: **Security**
   - Group name: `Enrolled Devices`
   - Membership type: **Dynamic Device**

- Owner: select the **No owners selected** link, then in the **Add Owners** window, select `Alex Wilber` and select **Select**.

5. Under **Dynamic device members**, click **Add dynamic query**.
6. On the **Dynamic membership rules** pane, configure the following fields for this expression:
   - Property: select the drop-down arrow and select **managementType**
   - Operator: select the drop-down arrow and select **Equals**
   - Value: enter `MDM`
7. Select the **Rule syntax** field. It should display the following rule:

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

37 Proceed to Exercise 3

38 Module 8 - Lab 1 - Exercise 3 - Creating compliance and conditional access policies

38.0.1 Scenario

Datum would like to ensure that enrolled Windows 10 devices meet a minimum configuration specification. The following are required:

- Minimum OS version: 10.0.17763.615
- Windows Defender Antimalware required
- iOS and MacOS platforms blocked

If the device does not meet these requirement, the device should be marked as non-compliant.

38.0.1.1 Task 1: Create and apply compliance policy and enrollment restrictions

1. Sign in to **LON-CL1** as **ADATUM\Administrator** with the password `Pa55w.rd`.
2. In Microsoft Edge, type `https://endpoint.microsoft.com` in the address bar, and then press **Enter**. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
3. From the navigation pane click **Devices**, then click **Compliance Policies**.
4. On the **Compliance policies | Policies** blade, in the details pane click **Create Policy**.
5. On the **Create a policy** blade, provide the following values and click **Create**:
   - Platform: **Windows 10 and later**
6. On the Basics tab, provide the following values and click **Next**:
   - Name: `Compliance1`
7. On the **Compliance settings** tab, click **Device Health** and review the available settings.
8. On the **Compliance settings** tab, expand **Device Properties**. In the **Minimum OS version** field, type `10.0.16299.15`.
9. On the **Compliance settings** tab, expand **System Security**. Scroll down and set the **Windows Defender Antimalware** setting to **Require**. Click **Next**.
10. On the **Actions for noncompliance** tab, note that the schedule to **Mark device noncompliant** is immediately. Review how you can configure the number of days after which the device is marked as noncompliant, and configuration additional actions. Click **Next**.
11. On the **Assignments** tab, under **Included groups**, click **+ Add groups**. Click `Enrolled Devices`, choose **Select**, and then click **Next**.

12. Click **Create**.
13. From the left menu click **Devices**, then click **Enroll devices**.
14. On the **Enrollment devices | Windows enrollment** blade, click **Enrollment restrictions**.
15. On the details pane, in the **Device Type Restrictions** section, on the **Default** line, click **All Users**.
16. On the **All Users** blade, click **Properties**. In the **Platform settings** section, click **Edit**.
17. On the **Platforms settings** tab, in the **Platform** column, on the rows with **iOS/iPadOS** and **macOS**, click **Block**. Click **Review + save** and then click **Save**.
18. Scroll left to the **Enrol devices | Enrollment restrictions** blade. In the **Device Limit Restrictions** section, click **All Users** and then click **Properties**.
19. In the **Device limit** section, click **Edit**, then change the value to **3**.
20. Click **Review + Save**, and then click **Save**.

38.1 Task 2: Creating a conditional access policy

38.1.1 Scenario

When devices are non-compliant, they should not be able to access their e-mail. You've been asked to configure a conditional access policy that enforces this rule, and verify it functions as expected.

1. On **LON-CL1**, in the **Microsoft Endpoint Manager admin center** click **Devices**, then click **Conditional Access**.
2. In the **Conditional Access | Policies** pane, click **+ New policy**.
3. On the **New** blade, in the **Name** text box, type `Conditional1` and then click **Users and groups**.
4. On the **Users and groups** blade, click the **All users** radio button.
5. On the **New** blade, click **Cloud apps or actions**, click the **Select apps** radio button, click **Select**, click **Office 365 Exchange Online**, and then click **Select**.
6. On the **New** blade, click **Conditions > Device platforms**. In the **Configure** section, click **Yes**, click the **Select device platforms** radio button, click the **Windows** check box, and then click **Done**.
7. On the **New** blade under **Access controls**, click **Grant**, click the **Require device to be marked as compliant** check box, and then click **Select**.
8. On the **New** blade, click **On** for the **Enable policy** option and then click **Create**.

38.1.1.1 Task 3: Verify that the conditional access policy is working

1. On **LON-CL2**, open a new Microsoft Edge tab, then and open `https://portal.office.com`.
2. Click the **Outlook** icon.
3. Verify that you receive the message **"You can't get there from here"** or similar warning message.
4. Click **More details**. You should see more information about why you are blocked. **Note:** This is because LON-CL1 is not joined to Azure AD and not managed by Intune, so not marked as compliant.
5. **Close** the browser window.
6. Return to **LON-CL1** and open EndPoint Manager. In Microsoft Edge, type `https://endpoint.microsoft.com` in the address bar, and then press **Enter**. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
7. Click **Devices** and then click **Conditional access**. Click the ellipses next to policy "Conditional1" and click **Delete**. Click **Yes** to confirm deletion. Note: If you don't delete this policy it will interfere with later labs.

End of lab

39 Module 9 - Lab 1 - Exercise 1 - Initialize Compliance

In your role as Holly Dickson, Adatum's Security Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, your next steps are to implement archiving and retention at Adatum.

39.0.1 Task 1 – Activate In-Place Archiving

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

1. Go to the Microsoft 365 compliance center. Click **Information governance** in the left pane (you might to click **... Show all** at the bottom before it appears). In the **Information governance** window, click the **Archive** tab.
2. On the **Archive** window, note that the archive mailboxes for all users other than Holly Dickson are enabled. These archive mailboxes were enabled when the VMs were built for this training course and these users were preconfigured in the tenant. However, since you added Holly in an earlier lab, her archive mailbox is disabled by default.
3. To enable Holly's archive mailbox, click the three vertical dots to the right of the name, then click **Enable archive** on the submenu that opens.
4. On the **Warning** screen that opens, click **Enable** to confirm.
5. Back on the **Archive** tab, click **Refresh** to see that the **Archive mailbox** status for Holly Dickson has changed to **Enabled**.

40 Proceed to Exercise 2

41 Module 9 - Lab 1 - Exercise 2 - Configure retention tags and policies

In this exercise, you will configure retention tags and policies, and you will implement archiving with MRM retention tags.

41.0.1 Task 1 – Create an MRM retention tag and policy in the Exchange Admin Center

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

1. On LON-CL1 virtual machine. In **Microsoft Edge**, navigate to the **Microsoft 365 admin center**.
2. In the **Microsoft 365 admin center**, in the left navigation pane, select **... Show all**.
3. In the left navigation pane, under **Admin centers** select **Exchange**. This will open the Exchange admin center.
4. In the **Exchange admin center**, in the left navigation pane, select **Classic Exchange admin center** and then **Compliance management**.
5. In the **Compliance management** window, select the **retention tags** tab that appears at the top of the page.
6. You want to create a retention tag, so select the **plus (+) sign** in the toolbar that appears across the list of existing retention tags. In the drop-down menu that appears, select **applied by users to items and folders (personal)**.
7. In **new tag applied by users to items and folders (personal)** window, under **Name**, type `3 Years Move - Archive after three years`.
8. Under **Retention Action**, select the **Move to Archive** option.
9. Under **Retention period**, select the **When the item reaches the following age (in days)** option, and type `1095` in the retention period field.
10. Under **Comment**, enter `Personal tag to archive email three years after being received`.

11. Select **Save**. Select **OK** once successful.
12. On the menu bar on the top of the page, select the **retention policies** tab.
13. You want to create a retention policy, so select the **plus (+) sign** in the toolbar that appears across the list of existing retention policies.
14. In **new retention policy** window, under **Name**, type **Office Retention Policy**.
15. Below **Retention tags**, select the (+) sign.
16. In the **select retention tags** window, select the tag that you just created, whose name starts with **3 Years Move...** (the column width will truncate the displayed name).
17. Select **add ->** and then select **OK**.
18. In addition to the personal retention tag that you just added to the retention policy, you also want to add the following default tags as well:
    - Default 2 year move to archive
    - Deleted Items
    - Junk Email
    - Recoverable Items 14 days move to archive

To add these tags, repeat steps 15-17. Hold down the **Ctrl** key as you select each tag in the list; this will enable you to select all four default tags at one time before selecting **add->**. Once complete select **OK**.

19. On the **new retention policy** window, select **Save**. Select **OK**.
20. In the **Exchange Admin Center**, in the left navigation pane, select **recipients**.
21. You are now going to apply this retention policy to the mailboxes for your two test users, Joni and Alex. In the list of recipient mailboxes, select **Joni Sherman** and then select the **pencil (edit) icon** in the toolbar to edit the properties of Joni's mailbox.
22. In the **Joni Sherman** properties window, select **mailbox features**.
23. On the **Warning** dialog box, select **OK**.
24. Select the drop-down arrow in the **Retention policy** field and select **Office Retention Policy**.
25. Select **Save** and then select **OK**.
26. Repeat the same steps for **Alex Wilber**.
27. Leave your web browser open and proceed to the next task.

You have now created a new retention policy with several retention tags, including a custom personal retention tag. Then you have assigned the retention tags via a retention policy to Alex and Joni's mailboxes.

41.0.2 Task 2 – Create a Retention Policy in the Security and Compliance Center

As part of your pilot project for Adatum, you will create a retention policy in the Security & Compliance Center to preserve the content of all Exchange Online mailboxes from deletion for 7 years after the last modification.

1. In **Microsoft Edge**, go to the Microsoft 365 compliance. Make sure that you are logged in as **Holly Dickson**.
2. In the left navigation pane, click **Information Governance** (you might need to click **... Show all** first) and then select the **Retention** tab.
3. In the **Retention** tab, click **+ New retention policy** to start the wizard that's used to create a new retention policy.
4. On the **Name your policy** page, type **Exchange Preservation** in the **Name** field and select **Next**.
5. In the **Choose locations** page, deselect all sliders except for **Exchange email.**. Click **Next**.
6. On the **Decide if you want to retain content, delete it, or both** page, leave the **Retain items for a specific period** option selected, and **7 years**. Do not change these fields. However, in the **Retain the content based on** field, it currently indicates **when it was created**. Select the drop-down arrow for this field and select **when items were last modified**.

7. Click **Next**.
8. On the **Review your settings** page, review all the settings. If any need to be corrected, select the **Edit** option and make the appropriate correction. Select **Submit** to finish the wizard.
9. Do not close your Client 1 VM or Microsoft Edge. Leave your web browser open as well as all tabs for the next lab.

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

42 End of Lab

43 Module 10 - Lab 1 - Exercise 1 - Configure Office 365 Message Encryption

In this lab, you will take on the persona of Holly Dickson, Adatum's Security Administrator. You have been tasked with piloting the use of Office 365 message encryption in Adatum's Microsoft 365 deployment.

In this exercise you will set up Azure Rights Management for your tenant. You will also learn how to create a mail flow encryption rule using the Exchange Admin Center.

43.0.1 Task 1 – Enable Azure Rights Management for Exchange Online

In this task you will activate Rights Management protection from the Microsoft 365 admin center.

1. Switch to the Client VM (**LON-CL1**). You should still be logged into LON-CL1 as **LON-CL1\Admin**, and you should still be logged into Microsoft 365 as **Holly Dickson**.
2. Open the Microsoft 365 admin center `https://admin.microsoft.com` if it's not already open on your browser.
3. Select **Settings** and then select **Org settings**.
4. On the Services tab select **Microsoft Azure Information Protection**.
5. In the Microsoft Azure Information Protection pane select **Manage Microsoft Azure Information Protection settings**.
6. You may be asked to sign-in again. If so login as Holly Dickson.
7. If rights management is not already activated select **activate**. You have now validated activation of rights management in your tenant.

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

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

1. On the **LON-CL1** VM, you should still be logged into the Microsoft 365 admin center as Holly Dickson. If you closed your Edge browser or the Microsoft 365 admin center tab, then in Microsoft Edge navigate to `https://portal.office.com` and sign in as Holly@M365xZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and `Pa55w.rd`.
2. In the **Office 365 home page**, select **Admin**.
3. In the **Microsoft 365 admin center** left navigation pane, select **Show all**, which expands the list of options in the navigation pane.
4. Scroll down in the navigation pane and under **Admin centers**, select **Exchange**. This will open the Exchange admin center.
5. In the **Exchange admin center**, in the left navigation pane select **mail flow.**
6. At the top of the **mail flow** page, the **rules** tab displays by default. In the **rules** tab, select the plus sign (+) to create a new rule. This displays a drop-down menu of actions. Select **Create a new rule.**
7. In the **new rule** window, in the **Name** box, enter `Encrypt mail for guest@contoso.com` as the name of this rule.

8. Select the drop-down arrow in the **Apply this rule if… ** condition box. In the drop-down menu, select **the recipient is**.
9. For this condition, you must either select an existing name from the contact list or type a new email address in the **check names** box. In this case, enter `guest@contoso.com` in the **Check names** box and then select **OK**.
10. You need to add more conditions, so select **More options**.
11. Select **add condition**.
12. Note how a second condition box appears below **The recipient is…** condition box. In this second condition box, select the drop-down arrow and select **The recipient**. Then in the drop-down menu select **is external/internal.**
13. In the **select recipient location** dialog box, select the drop-down arrow. In the drop-down menu, select **Outside the organization** and then select **OK**.
14. You now need to define an action to perform when this rule is applied. In the **Do the following…** box, select the drop-down arrow. In the drop-down menu, select **Modify the message security….** In the menu that appears, select **Apply Office 365 Message Encryption and rights protection.**
15. In the **select RMS template** dialog box, select the drop-down arrow, select **Encrypt**, and then select **OK.**
16. Select **Save.** Once the rule is saved, it should appear in the list of rules in the Exchange admin center.
17. Leave your browser session open for the next exercise.

44 Module 10 - Lab 1 - Exercise 2 - Validate Information Rights Management

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

44.0.1 Task 1 - Validate Information Rights Management for Exchange Online

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

1. On the Client 1 VM (**LON-CL1**), you should still be logged into the Microsoft 365 admin center as Holly Dickson. In your **Microsoft Edge** browser, you should still have the **Office 365 home** page open on a tab. Select the **Office 365 home page** tab, and then select **Outlook.** **Note**: If you are prompted to select a time zone, then choose one and select **Save**.
2. At the top of the left navigation pane, select **New message** to create a new email.
3. You want to send the email to **Alex Wilber**. Type **Alex** in the **To** field, which displays a dialog box that displays all users whose Display Name starts with Alex (of which there is just one). Select **Alex Wilber**.
4. Enter a **Subject**, and then type some text in the message body.
5. In the menu bar above the message pane, select **Encrypt**.
6. The message will now have a lock icon and list it as encrypted. To the right of the lock icon select **Change permissions**.
7. In the Change permissions window click the drop-down and select **Do not forward**. Select **OK**.
8. Select the **Send arrow** to send the email.
9. Switch to the Client 2 VM (**LON-CL2**).
10. On the taskbar, select the **Microsoft Edge** icon. In your **Edge** browser navigate to `https://portal.office.com`. In the **Pick an Account** window, if **Alex Wilber** is listed then select his username; otherwise, select **Use another account** and log in as AlexW@M365xZZZZZZ.onmicrosoft.com (where ZZZZZZ is

your unique tenant ID provided by your lab hosting provider) his password is probably the same as the MOD admin password for your tenant as set by your lab provider.

11. In the **Office 365 home page**, select **Outlook**.
12. On the **Outlook** page, select your **language** and **time zone** and select **Save**.
13. If a **We've updated Outlook** window appears, select **Try the new Outlook**.
14. If a **Welcome** window appears, close it.
15. Verify that Alex received an email from Holly that is IRM protected. IRM protected emails display a lock icon to the right of the message. Select the message to display it in the right pane.
16. In the message pane for this email, a message that says **This messsage is encrypted and recipients can't forward it** should appear.
17. In the message pane for this email, note how the **Forward** arrow is disabled.
18. Select the **ellipsis icon (More actions)** to the right of the disabled Forward arrow. In the menu that appears, note how both the **Forward** and **Print** options are disabled.
19. In your **Edge** browser, close the **Outlook** tab.
20. You want to remain logged into the Office 365 home page as **Alex Wilber** on **LON-CL2** for the next task, so leave the **Office 365 home page** tab open and proceed to the next task.

44.0.2 Task 2 - Validate Information Rights Management for SharePoint Online

In first lab of this course, you enabled Information Rights Management for Adatum in SharePoint Online.

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

1. Switch to the **LON-CL1** VM where you should still be logged into the Microsoft 365 admin center as Holly Dickson. If not go to `https://portal.office.com` and select **Admin**.
2. The **SharePoint admin center** tab should still be open in your browser from Lab 1 when you enabled IRM for SharePoint Online; if so, select this tab now. However, if you closed this tab, then In the **Microsoft 365 admin center**, scroll down through left-hand navigation pane and under **Admin centers**, select **SharePoint**. This will open the SharePoint admin center.
3. In the **SharePoint admin center**, in the left navigation pane, select **Sites**, then **Active sites**.
4. On the **Active sites** page, select the **+ sign** to **Create**.
5. Scroll down to **Other options** then in the **Choose a template** drop down box choose **More Templates**
6. On the **Create site collection** window, enter the following attributes:
   - Title: `Marketing`
   - Web Site Address: leave the default values in the two drop-down fields. In the field to the right of the drop-down field with **/sites/** displayed, enter `marketing`.
   - Language: select your language
   - Select a template: leave the default value of **Team site (classic experience)** as the selected value
   - Time zone: select the appropriate time zone in which the team site is located
   - Administrator: Enter **Holly@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and then select the **Check Names** icon to the right of the field; once the username is validated, it will be replaced with **Holly Dickson.**
   - Server Resource Quota: leave the default value of 300
7. Select **OK**.
8. Wait for the new SharePoint site to be created, which may take up to 15 minutes. The new Marketing site collection will appear in the **Active sites** collection list, but the "Processing" circle will continue to spin to the right of the site collection while it continues being created.
9. Once the Marketing site collection is created, **New** will appear to the right of the site collection.

10. In your web browser, open a new tab and connect to: `https://M365xZZZZZZ.sharepoint.com/sites/marketing` (where ZZZZZZ is your tenant ID provided by your lab hosting provider)
11. On the **Marketing** site, in the left navigation pane, select **Documents**.
12. In the **We've got a new look** window, if it appears, select **NOT NOW**.
13. In the **Documents** page for the **Marketing** site, at the top right, select the **gear** (**Settings)** icon and then select **Library settings**.
14. On the **Documents>Settings** page, under **Permissions and Management**, select **Information Rights Management**.
15. On the **Information Rights Management Settings** page, select the **Restrict permissions on this library on download** checkbox.
16. In the **Create a permission policy title** box, type `Marketing Policy`.
17. In the **Add a permission policy description** box, type `Marketing policy for downloads`.
18. Select **SHOW OPTIONS**.
19. Under **Configure document access rights**, select the **Allow viewers to write on a copy of the downloaded document** checkbox and select **OK**.
20. In the top-right corner of the page, select **Share**.
21. In the **Share 'Marketing'** window, in the **Invite people** box, enter `Alex Wilber`. Select **Alex Wilber** that appears in a drop-down menu, and then select **Share**.
22. Now that Holly has created this new SharePoint site and used IRM to restrict permissions on the site, she has asked Alex Wilber to test this site to validate whether IRM is working for SharePoint Online. Alex will perform this test on the Client 2 (**LON-CL2**) VM.

    Switch to the **LON-CL2** VM, where you should still be logged into the Microsoft 365 admin center as Alex from the prior task.
23. In the **Microsoft Edge** browser on LON-CL2, open a new tab and enter the following URL in the address bar to navigate directly to the Marketing site: `https://M365xZZZZZZ.sharepoint.com/sites/marketing` (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider)
24. In the **Pick an Account** window, select **Alex Wilber** if his account is listed; otherwise, select **Use another account** and log in as **AlexW@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) the password is likely the same as your MOD admin assigned by your lab hosting provider.
25. On the **taskbar of your VM**, select the **Search** icon and type **WordPad** in the Search field. Select **WordPad** that's displayed.
26. In the WordPad window, enter some text for a new test document.
27. Select **File** and **Save**. In the **Save As** window, under **This PC**, select **Desktop.** Type `TestDocument` in the **File name** field, and in the **Save as type** field, select **Office Open XML Document (*.docx)**.
28. Close WordPad.
29. Select **Documents** on the left pane in SharePoint.
30. On the **Documents** page, in the menu bar, select **Upload**, and then in the drop-down menu select **Files**.
31. In the **File Explorer** window, select **Desktop** under the **Quick access** section, select **TestDocument.docx**, and then select **Open**. This will upload the file to the **Documents** page in the **Marketing** site collection.
32. In the list of Documents, right-click on **TestDocument.docx**, select **Open**, and then select **Open in browser**.
33. Verify that the **Marketing Policy** displays in a warning message at the top of the page.
34. Try to enter some text in the document. Verify that Alex cannot edit the document in Word Online because it's protected in this site collection. A Read-only information line will display at the top of the page indicating the document is read-only.
35. Leave your browser open for the next lab.

45 End of Lab

46 Module 11 - Lab 11 - Exercise 1 - Manage DLP Policies

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

46.0.1 Task 1 – Create a DLP policy with custom settings

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

1. You should still be logged into your Client 1 VM (**LON-CL1**) as the **LON-CL1\Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In **Microsoft Edge**, the Office 365 Security & Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to `https://protection.office.com`.
3. In the **Security & Compliance Center**, in the left navigation pane, select **Data loss prevention** and then select **Policy**.
4. In the **Policy** window, select **+Create a policy** to start the wizard for creating a new data loss prevention policy.
5. On the **Start with a template or create a custom policy** page, you want to select **Custom** in the left pane and **Custom policy** in the middle pane; however, by default, both these options should already be selected (if not, then select them now), so simply select **Next**.
6. In the **Name your policy** page, type `Social Security DLP Policy` in the **Name** field and `Protect social security numbers from being shared` in the **Description** field. Select **Next**.
7. On the **Choose locations** page, select the **Protect content in Exchange email, Teams chats, and channel messages and OneDrive and SharePoint documents** option and then select **Next**.
8. On the **Customize the type of content you want to protect** page, the option **Find content that contains:** needs to be selected, which it should be by default.
9. Under **You must select at least one classification type**, select **Edit.**
10. In the **Choose the types of content to protect** page, select the **Add** drop-down field, and in the drop-down menu, select **Sensitive info types**.
11. In the Sensitive info types window, select **(+) Add**.
12. In the search field type `social` and wait until the search results are displayed.
13. In the list of search results, select the **U.S. Social Security Number (SSN)** check box, and then select **Add**.
14. Once you receive the message indicating **1 sensitive info type added,** select **Done**.
15. On the **Choose the types of content to protect** window, under the **Content contains** bar, select **Any of these** in the drop-down field (this should be selected by default), and then select **Save**.
16. On the **Customize the type of content you want to protect** page, **U.S. Social Security Number (SSN)** should now appear under the **Find content that contains** option.
17. Verify that the **Detect when this content is shared:** check box is selected.
18. In the field below this, select the drop-down arrow and select **only with people inside my organization**.
19. Select **Next**.
20. On **What do you want to do if we detect sensitive info?** page, check that **Detect when content that's being shared contains** is selected. In the field below this, **10** is entered. Change this to **2**.

21. Notice that **Send incident reports in email** is marked and **Block people from sharing and restrict access to shared content** is marked. This configuration means that if Microsoft DLP detects 2 or more US Social Security numbers present in an email, the email will not be delivered and a report will be sent to you and your global admin. Once you confirm these settings select **Next.**
22. On the **Customize access and override permissions** page, select **Next**.
23. On the **Do you want to turn on the policy or test things out first?** page select **Yes, turn it on right away** and select **Next**.
24. Check the configuration on the **Review your settings** page, select **Back** if you need to correct any settings, and then select **Create** once you're satisfied with the settings.

You have now created a DLP policy that scans for US Social Security numbers in emails and documents that are sent or shared in your organization.

47 Proceed to Exercise 2

48 Module 11 - Lab 1 - Exercise 2 - Test DLP Policies

You are now at the point in your pilot project where you want to test policies. You have decided to test a DLP policy related to emails that contain sensitive information.

48.0.1 Task 1 – Test a DLP Policy for Sensitive Emails

In the previous exercise, you created a custom DLP policy that searches emails for sensitive information related to U.S. Social Security numbers in your Adatum tenant. In this exercise, you will send an email with a social security number from Holly Dickson to Alex Wilber.

1. Switch to the Client 1 VM (**LON-CL1**), in which you should still be logged into Microsoft 365 as Holly Dickson (holly@M365xZZZZZZ.onmicrosoft.com) with a password of `Pa55w.rd`.
2. You will now send an email from Holly to Alex; the email will contain US Social Security numbers. In **Microsoft Edge**, the **Outlook on the web** tab should still be open for Holly. Select the **Outlook on the web** tab. If not open a browser to `https://portal.office.com`, make sure you are signed-in as Holly Dickson and select **Outlook**.
3. In the upper left corner of the screen, select **New message**.
4. In the message pane that appears on the right-side of the screen, enter the following information:
   - To: start typing `Alex` and a drop-down menu displays with users whose name begins with that. Select **Alex Wilber**.
   - Add a subject: `DLP Policy Test`
   - Message area: type `This customer has social security number: 123-45-6789`.
5. Select **Send.**
6. You will now send a second message from Holly to Alex that contains multiple social security numbers. In **Outlook**, in the upper left corner of the screen, select **New message**.
7. 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 that. Select **Alex Wilber**.
   - Add a subject: `multiple SSN test`
   - Message area: `SSN = 123 45 6789 and another customer SSN 111 11 1111 and a third 222 22 2222`
8. Select **Send.**
9. Switch to the Client 2 VM (**LON-CL2**).
10. If you need to sign into the VM, the **Admin** account should appear by default, so enter `Pa55w.rd` in the **Password** field to log in.
11. Switch to the Client 2 VM (**LON-CL2**).

12. In the **Edge** browser, if there are still signed in sessions, sign out of the current user account and close all **Edge** browser tabs.

13. Open your **Edge** browser, maximize the window and enter the following URL in the address bar: `https://outlook.office365.com`

14. You want to sign into **Outlook on the web** as **Alex Wilber**. If the **Pick an account** window appears, Alex's account won't appear since she hasn't signed in before. Therefore, select **Use another account**.

15. In the **Sign in** window, enter **AlexW@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) and then select **Next.**

16. In the **Enter password** window, enter Alex's password (hint: it's probably the same as the MOD admin password) and then select **Sign in**.

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

18. If you approach the site for the first time, you may be asked for your language setting and your time zone:

    - From the **Language** dropdown select **English (United States).**
    - From the **Time zone** dropdown select your preferred time zone.

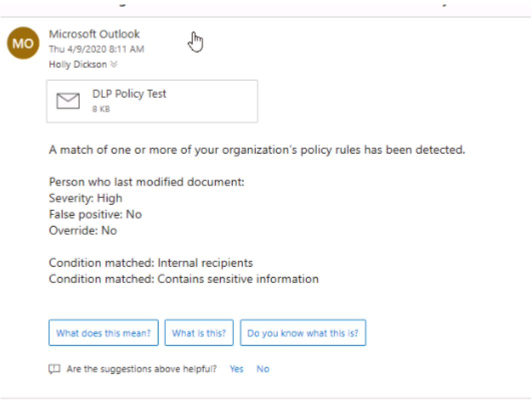
19. Select **Save**.

20. If a window is displayed asking whether you want to try the new outlook, select **Try the new Outlook.**

21. If a **Welcome** window appears, then close it now.

22. In **Outlook on the web**, in Alex's **Inbox**, you should see the email message that Holly just sent to Alex containing a single SSN number.

23. The email with multiple SSNs should have been blocked and a warning message should appear in Holly's inbox (on LON-CL1) that looks something like this:



Microsoft Outlook
Thu 4/9/2020 8:11 AM
Holly Dickson

DLP Policy Test
8 KB

A match of one or more of your organization's policy rules has been detected.

Person who last modified document:
Severity: High
False positive: No
Override: No

Condition matched: Internal recipients
Condition matched: Contains sensitive information

MO
What does this mean?
What is this?
Do you know what this is?
Are the suggestions above helpful? Yes No

24. Delete the message from Alex's Inbox as the last operation in this exercise. You have now successfully tested your custom DLP policy.

25. Leave both client VMs open for the next lab. Do not close any of the browser tabs.

TROUBLESHOOTING this lab

"Nothing happened, both emails went to Alex".

1. It can take many minutes for a DLP policy to propagate a tenant. Most likely you sent the emails to Alex before the policy and subsequent scanning had a chance to be in place in your tenant. If that happened come back to this lab later and resend the emails again.

2. Another possibility is that you didn't format the SSN's properly in the body of the email. Sensitive information types in DLP policies scan for data formatted in a particular way that is common for that data type. If you click the link below you can see exactly how US Social Security numbers must be formatted in content in order to be detected by DLP policy scans. https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-sensitive-information-types-look-for?view=o365-worldwide#us-social-security-number-ssn

3. Check the DLP Policy configuration. Make sure you configured the policy as described in the previous exercise.

This is a good lab for testing various DLP policy configurations. Once you have successfully completed this lab consider reconfiguring this DLP policy to trigger other outcomes.

49 End of Lab

50 Module 13 - Lab 1 - Exercise 1 - Set up privileged access management and process a request

In your role as Holly Dickson, Adatum's Security Administrator, you have been tasked with establishing privileged access management in Microsoft 365 as an additional layer of access management for global admins. Specifically, Adatum wants to prevent global admins from moving Exchange Mailboxes without getting specific approval from the MOD Administrator.

In this exercise, you will set up Privileged Access Management and create an access policy.

50.0.1 Task 1 – Create an approver's group

Before you start using privileged access, determine who needs approval authority for incoming requests for access to elevated and privileged tasks. Any Global Admin who is part of the Approvers' group is able to approve access requests. Adatum has decided to make the MOD Administrator, the user who will approve access requests.

1. You should still be logged into your Client 1 VM (**LON-CL1**) as the **LON-CL1\Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, if you have the **Microsoft 365 admin Center** open in a tab, then select it; otherwise, open a new tab and enter the following URL in the address bar: `https://admin.microsoft.com`.
3. In the admin center, click **Groups** and then select **Active Groups**. In the **Active Groups** screen select **Add a group**.
4. In the **Choose a group type** screen select **Mail-enabled security** and select **Next**.
5. In the **Set up the basics** screen enter the Name `Privileged Access Approval Group` and enter a similar description and then select **Next**.
6. In the **Edit settings** screen for the group email alias type **access**, tab to the next field to ensure it's acceptable, then select **Next**.
7. In the **Review and finish adding group** screen select **Create group**. Select **Close**.
8. In the **Active Groups** screen select the group you just created. You may have to click **refresh** after several minutes for the group to appear in the list.
9. In the **Privileged Access Approval Group** screen click the **Members** tab and then select **View all and manage members**.
10. Select **+ Add members** search for `MOD Administrator`. Select MOD Administrator and click **Save**. Click **Close** twice to return to the **Groups** screen.

Note: Holly Dickson is listed as the owner of the group you just created. She is therefore part of the Privileged Access Approval Group. In practice, and to support the scenario, you would make MOD Administrator the owner of the group and leave Holly out of it to prevent her from being able to approve her own privileged access requests.

50.0.2 Task 2 – Enable privileged access

1. In the Microsoft 365 admin center, signed in as global administrator Holly Dickson. Select **Settings** then select **Org settings**.
2. In the Org settings screen select the **Security & privacy** tab and then select **Privileged access**.
3. In the Privileged Access screen make sure **Allow Priviledged access requests and choose default approval group** is **Checked**.

4. Select the **Privileged Access Approval Group** as the **Default approval group**. Click **Save** and **Close**.

50.0.3 Task 3 - Create a privileged access policy

It has been decided that Exchange mailbox moves tasks will require privileged access approval for Global Admins to complete such tasks. In this task you will configure this policy.

1. In the Microsoft 365 admin center, signed in as global administrator Holly Dickson. Select **Settings** then select **Org settings**.
2. In the Org settings screen select the **Security & privacy** tab and then select **Privileged access**.
3. In the Privileged Access screen select **Create policies and manage requests**.
4. Select **manage policies** and then select + **Add a policy**.
5. In the **Add Policy** window select the following:

Policy type = **Role**

Policy scope = **Exchange**

Policy name = **Move Mailboxes**

Approval type = **Manual**

6. Select the **Privileged Access Approval group** as the **Approvers** and select **Create**. Select **Close**

50.0.4 Task 4 - Submit a request for privileged access.

In this task you will request access to the Compliance Admin role to attain temporary access to perform certain Compliance actions.

1. In the Microsoft 365 admin center, signed in as global administrator Holly Dickson. Select **Settings** then select **Org settings**.
2. In the Org settings screen select the **Security & privacy** tab and then select **Privileged access**.
3. In the Privileged Access screen select **Create policies and manage requests**.
4. Select **Access Requests** Then + **Request Access**. In the **Request Access** screen select the following and then **Create**

Request type: **Role**

Request scope: **Exchange**

Request for: **Move Mailboxes**

Duration(hours): `8`

Comments: `I need to move mailboxes for the new department today.`

5. When the access request is done processing select **Close**

50.0.5 Task 5 - Approve a privileged access request.

1. Switch to **LON-CL2** virtual machine. In the Microsoft 365 admin center (`https://admin.microsoft.com`), sign in as **MOD Administrator** the password for this account was assigned by your lab hosting provider. Select **Settings** (you may need to click **... Show all** first) then select **Org settings**.
2. In the Org settings screen select the **Security & privacy** tab and then select **Privileged access**.
3. In the Privileged Access screen select **Create policies and manage requests**.
4. By default the **All Requests** view should display all Privileged Access Requests.
5. Select the request for **Move Mailboxes** access with the status of **Pending**.
6. In the **Compliance Admin** screen select **Approve**. Select **Close**.

Summary: Global Admin Holly Dickson required short-term authorization to move mailboxes. She requested 8 hours of access to those role tasks which was approved by the MOD Administrator.

Important: It would be prudent to disable Privileged Access Management after completing this lab so it doesn't accidentally interfere with actions in the remaining labs.

51 Module 14 - Lab 1 - Exercise 1 - Investigate Your Microsoft 365 Data

In your role as Holly Dickson, Adatum's Security Administrator, you have Microsoft 365 deployed in a virtualized lab environment. As you proceed with your Microsoft 365 pilot project, you now want to test how Adatum can investigate its Microsoft 365 data. You have decided to focus on performing a content search for deleted emails, which is a common request at Adatum, and then you want to analyze eDiscovery functionality by creating an eDiscovery case. You will conclude this portion of the pilot project by creating a GDPR data subject request.

51.0.1 Task 1 – Perform a content search for deleted emails

In this exercise, you will add Joni Sherman and Holly Dickson as members of the eDiscovery Manger role, and then you will log into the Client VM as Joni and perform a content search that looks for emails with the keywords related to social security numbers.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Holly Dickson**.
2. In your **Microsoft Edge** browser, if you have the **Security and Compliance Center** open in a tab, then select it; otherwise, open a new tab and enter the following URL in the address bar: `https://protection.office.com`.
3. In the **Office 365 Security and Compliance Center**, in the left navigation pane, select **Permissions.**
4. In the **Home > Permissions** page, select the **eDiscovery Manager** check box.
5. In the **eDiscovery Manager** role group window, scroll down to the **eDiscovery Manager** section and select **Edit**.
6. The **Editing Choose eDiscovery Manager** wizard opens. The list should be empty. Select **Choose eDiscovery Manager**.
7. In the **Choose eDiscovery Manager window**, select **(+) Add**.
8. In the list of users that's displayed, select `Joni Sherman` and `Holly Dickson`, and then select **Add**.

   Note: You are adding Joni to the eDiscovery Manager role group for later use in this exercise, and you are assigning Holly to the role group for use in the next exercise.
9. You should see a banner with the message **2 members added**. Select **Done** and then **Save**.
10. Switch to the Client 2 VM (**LON-CL2**). You should still be logged into **LON-CL2** as the **LON-CL2\Admin** account, and log into Microsoft 365 as **Joni Sherman**. In the **Sign in** window, enter **JoniS@M365xZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Select **Next**. In the **Enter password** window, enter Joni's password (hint: it is probably the same as the MOD password assigned by your lab hoster).
11. If you have a tab open in your **Edge** browser for the **Office 365 Security and Compliance Center**, then select it now. Otherwise, select a new tab and enter the following URL in the address bar: `https://protection.office.com`.
12. In the **Security and Compliance Center**, in the left navigation pane, select **Search**, and then under it select **Content search**.

    Note: If you cannot see **Search** in the navigation pane yet, you need to reload the browser tab with the **Security and Compliance Center.**
13. On the **Content search** window, in the **Searches** tab, select **(+) Guided search** on the top menu. This will initiate the **New search** wizard.
14. On the Name your search page, enter `Content Search Test` into the **Name** field and then select **Next**.
15. On the Locations page, select **All locations** and then select **Next**.

16. On the **Condition card** page, enter **SSN** press enter and type **social** into the **Keywords** box. Pressing enter between keywords will separate the words as independent terms in the list. Once the two terms are added select **Finish**.
17. Back on the **Searches** tab, the Search query will run. The Status field in the bottom-left corner of the screen will indicate when the query is complete. It may take many minutes for the query to run and the data to be displayed in the right pane. When the content search finishes, you will see all mailbox items that you have created for the sensitive information test of your custom DLP policy.

If you didn't send emails during the DLP lab earlier in the course then no data will appear in this search. If this happened, while the search is running, you could switch back to **LON-CL1** and send emails with the keyword terms mentioned in this lab to other users in your tenant. You may have to run this search again to view data if you do that.

You can let the search run while you proceed with the remainder of this exercise.

18. Leave the Client 2 VM open as well as all browser tabs and continue with the next task.

You have successfully assigned an eDiscovery role to Joni and performed a content search for a specific key word across all locations of your tenant.

51.0.2 Task 2 – Create an eDiscovery case

In this task, you will create an eDiscovery case with a configured hold and content search for any violations regarding social security numbers. You will continue using Joni Sherman's user account. Having been assigned the eDiscovery Managers role in the prior task, Joni has the permissions necessary to create an eDiscovery case.

1. You should still be logged into your Client 2 VM (**LON-CL2**) as the **LON-CL2\Admin** account and signed into Microsoft 365 as Joni Sherman. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign into Joni's **JoniS@M365xZZZZZZ.onmicrosoft.com** account using her password assigned by your lab hoster.
2. The **Security and Compliance Center** should still be open in a tab in Microsoft Edge. If so, select that tab now. If not, then enter the following URL in the address bar: `https://protection.office.com`.
3. In the **Security and Compliance Center**, in the left navigation pane, select **eDiscovery**, and then under it, select **eDiscovery**.
4. On the **eDiscovery** window, select **(+) Create a case** on the top menu.
5. In the **New case** window, enter `Social Security Violation` into the **Case name** field and select **Save**.
6. Back on the **eDiscovery** page, select **Open** that appears to the left of the **Social Security Violation** case.
7. On the **Social Security Violation** window, select the **Holds** tab from the top menu.
8. Select **(+) Create** to create a new hold. This initiates the **Create a new hold** wizard.
9. On the **Name your hold** page, enter `Social Security Violation - Content` into the **Name** field and then select **Next**.
10. On the **Choose locations** page, For the location **Exchange email**, select the **Choose users, groups or teams** field.
11. On the **Exchange email** page, select **Choose users, groups, or teams**.
12. Enter **Holly** into the search field, select the Search icon on the right side of the field.
13. Scroll down on the page, and under **Users, groups, or teams**, select **Holly Dickson** from the search results.
14. Select **Choose** and then select **Done**.
15. On the **Choose locations** page, **1 user, group, or team** is displayed to the right of **Exchange email**. Select **Next**.
16. On the **Query conditions** page, enter **SSN** press enter and then type **social** into the **Keywords** box. This will search for those two terms independently. Then select **Next**.
17. On the **Review your settings** page, review the values and select **Edit** next to any that need to be modified. When you are satisfied with the settings, select **Create this hold**, then select **Close**.

18. Back on the **eDiscovery Case overview**, on the **Social Security Violation > Core ED > Hold** page, select the **Searches** tab from the top menu.
19. Select **(+) New search.** and then in the drop-down select **(+) New search.**.
20. In the **New search** window, in the **Search query** pane on the left, enter `SSN` press enter and then type `social` in the **Keywords** field and then under **Locations**, select **Locations on hold**.
21. Select **Save & run**.
22. In the **Save search** window, enter `Social Security Violation - Search` into the **Name** field and then select **Save**.
23. This will initiate a search query that looks for the keywords **SSN**. Once the query is finished, wait for the preview results to be displayed.

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

52 Proceed to Exercise 2

53 Module 14 - Lab 1 - Exercise 2 - Conduct a Data Subject Request

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

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

53.0.1 Task 1 – Create a GDPR Data Subject Request

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

1. You should still be logged into your Client 1 VM (**LON-CL1**) as the **LON-CL1\Admin** account, and you should be logged into Microsoft 365 as **Holly Dickson** (**holly@M365xZZZZZZ.onmicrosoft.com**) with a password of **Pa55w.rd**.
2. In your **Microsoft Edge** browser, if you have the **Security and Compliance Center** open in a tab, then select it; otherwise, open a new tab and enter the following URL in the address bar: `https://protection.office.com` .
3. In the **Security and Compliance center**, in the left navigation pane select **Data privacy**, and then under it select **Data subject requests**.

Note: To perform this task, Holly needs to be assigned to the eDiscovery Manager role group so that she has the necessary permissions. You added Holly to this role group in the prior exercise at the same time that you added Joni Sherman to the role group. The reason we did this is explained below following the search query.

4. In the **Data subject requests** window, select **+New DSR case**. This initiates the New DSR case wizard.
5. In the **Name your case** page, enter the following information and then select **Next**:
   - Name: `Holly Dickson Subject Request`
   - Description: `This is a test of the Data Subject Request resource to pulling information on the subject Holly Dickson`.
6. In the **Request details** page, select the **Data subject (the person who filed this request)** field, which displays a list of users. Select **Holly Dickson** and then select **Next**.
7. In the **Confirm your case settings** page, review your settings. If necessary, select **Edit** next to either setting to change it. Once you're satisfied with the settings, select **Save**.

8. In the **Successfully created new DSR case** window, select **Show me search results**.
9. A new **Search query** window will appear and begin the query. In the bottom left corner of the screen, the status of the query is displayed. Wait for the status to show **Completed** this may take several minutes.

Note: The reason why you were instructed to add Holly to the eDiscovery Manager role group in the prior exercise rather than at the start of this one is that it takes several minutes for permissions to successfully propagate. If you had assigned Holly to this role group just prior to this query, you would have received error messages involving parameter fields because her permissions would not have completed propagating. By adding Holly to this role group in the prior exercise, enough time should have elapsed between then and now for the propagation to complete. If you still receive any error messages, click **OK** to resume the query. If this occurs, the query will not display any data.

Note: Depending on how much data is accrued, a query can take some time to complete. For Adatum's pilot project, they have not accrued much in terms of data, so Holly Dickson's query should only take a few minutes or so to complete.

10. At any point, scroll down under **Search query** in the left pane to review the default query parameters. You can modify any of the parameters and save the query for future use.
11. Select **Save** to save this DSR query for **Holly Dickson**.
12. Select the **Home** tab. For Holly Dickson's case, select **Close case** to the right of the Active status, and then select **Yes** on the **Warning** message.
13. Select the **Searches** tab again and open the saved search in the right pane by selecting **Holly Dickson Subject Request**.
14. In the **Holly Dickson Subject Request** window, scroll to the bottom of the window to view search statistics of the results as well as the search query syntax.
15. Leave this **Holly Dickson Subject Request** window open as you will resume testing in the next task from this point.

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

53.0.2 Task 2 – Export the DSR Search Query Results

When someone files a DSR, you typically need to export the results. In this task, Holly will export the DSR report for the previous case for further processing.

1. The **Holly Dickson Subject Request** window should still be open after having finished the previous task. In this window, select **More > Export report** at the top of the page.
2. In the **Export report** window, select the option that states: **All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons**.
3. Scroll down through the **Export report** window to see the estimated items that will be exported.
4. Select **Generate report**.
5. If a **Client Error** dialog box appears it may be a result of the search still running, select **OK** and wait for the search to complete to generate the report again.
6. Select the **Exports** tab from the top menu and open the **Holly Dickson Subject Request_ReportsOnly** export request.
7. In the right pane select **Download report** and when the download bar appears at the lower end of your browser, select **Open**.
8. An **Application Install – Security Warning** window will appear that wants to install the **Microsoft 365 Office 365 eDiscovery Export Tool**. Select the **Install** button.
9. When the **eDiscovery Export Tool** is installed, you need to copy the unique export key to the first text field. Go back to the **Holly Dickson Subject Request_ReportsOnly** export request in your browser window and below **Export key**, select **Copy to clipboard**.
10. Switch back to the **eDiscovery Export Tool** and paste the export key (press Ctrl+V) into the first text field.

11. Select the **Browse** button and in the **Browse For Folder** window, navigate to **Documents**. Select **OK**.
12. Start the export process by selecting **Start**.
13. As soon as the **eDiscovery Export Tool** shows three green checkmarks with a **The export completed successfully.** message below, the export is done, and you can view the results by opening the blue link next to **Export Location**.
14. You can now see a **results.csv** file that contains a report about all DSR case items found.
15. Close the **eDiscovery Export Tool** with the **Close** button, and then close the **eDiscovery** browser tab.
16. Leave **Holly** signed in at the **Security & Compliance Center**.

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

The reason we chose to perform the Data Subject Request on Holly Dickson is because she was involved in almost every lab in this course and thus would have significant data to appear in the final report at this time.

54 End of Lab