NAME: BINYANYA DEBORAH NYATICHI

CS NO: ADC-CSS02-25051.

DESCRIPTION: Week 3 Assignment 5

ASSIGNMENT: Lab on Describe the capabilities of Microsoft Security Solutions

DATE: 02/05/2025

INTRODUCTION

This week, I will be working on a series of labs designed to help me explore the capabilities of Microsoft Security Solutions. I will begin by setting up a Microsoft 365 tenant, which will provide the foundation for testing and configuring various security features. I will then explore tools such as Azure Network Security Groups (NSGs), Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender for Cloud Apps, and the Microsoft Defender portal. Through these labs, I aim to gain hands-on experience in managing cloud security, monitoring threats, and understanding how Microsoft's integrated tools work together to protect enterprise environments.

LAB: EXPLORE MICROSOFT DEFENDER FOR CLOUD APPS

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the threat protection capabilities of Microsoft 365
- Unit: Describe Microsoft Defender for Cloud Apps

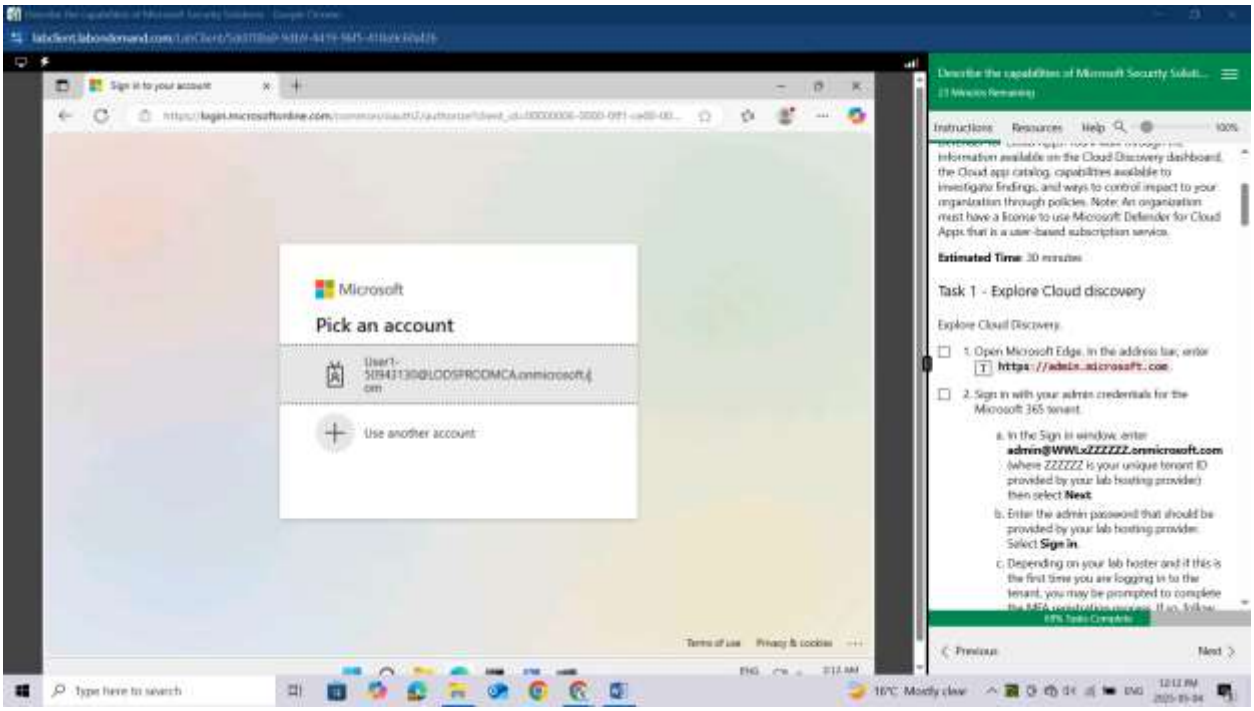
Lab scenario

In this lab, you'll explore the capabilities of Microsoft Defender for Cloud Apps. You'll walk through the information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies. Note: An organization must have a license to use Microsoft Defender for Cloud Apps that is a user-based subscription service.

Task 1 - Explore Cloud discovery

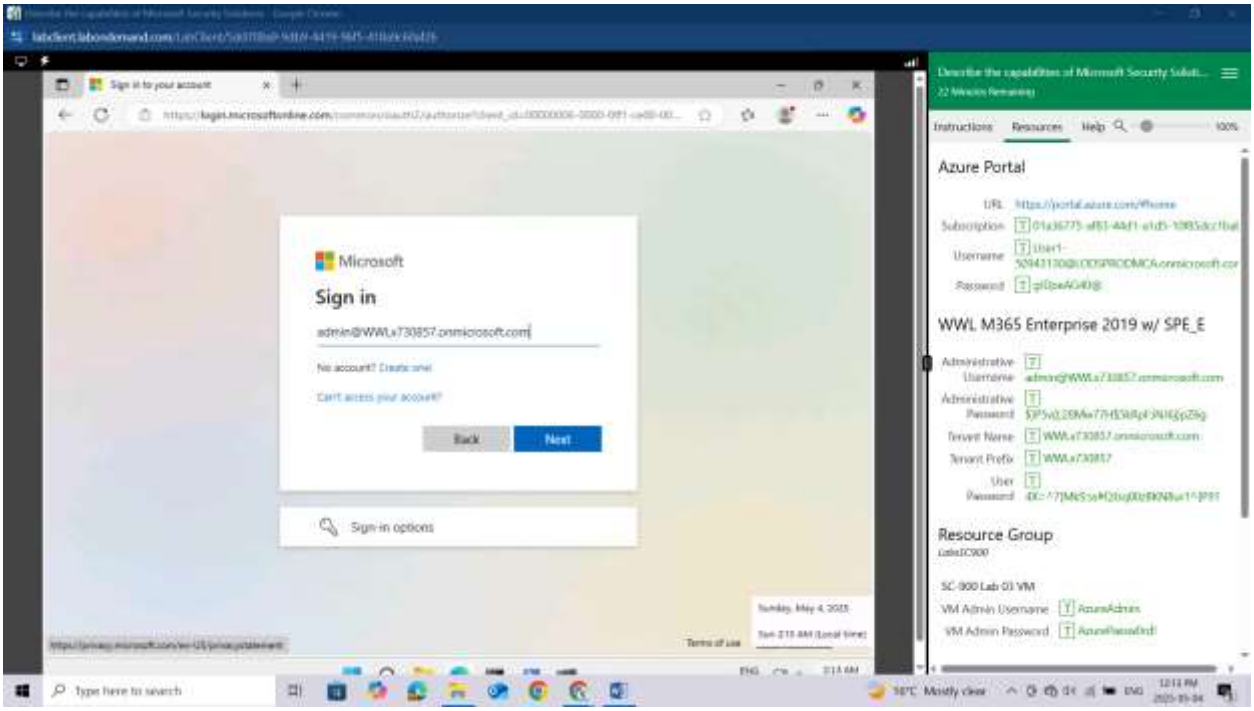
Explore Cloud Discovery.

Open Microsoft Edge. In the address bar, enter https://admin.microsoft.com.

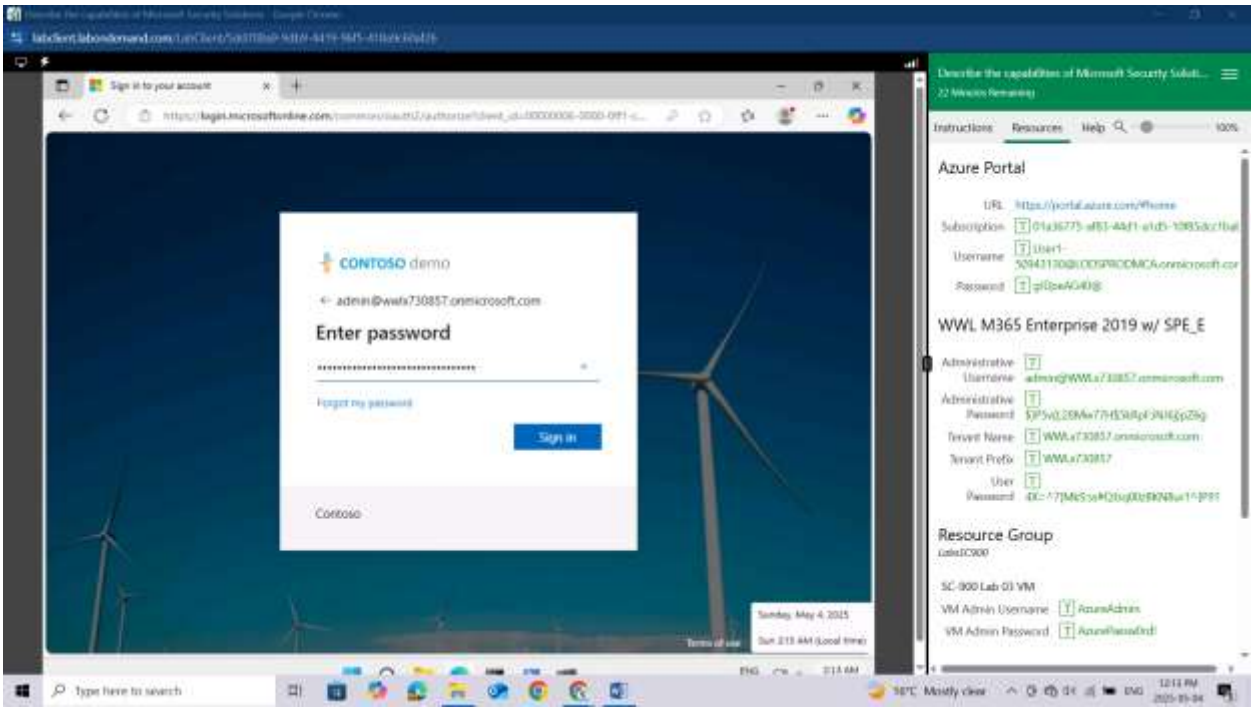


Sign in with your admin credentials for the Microsoft 365 tenant.

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

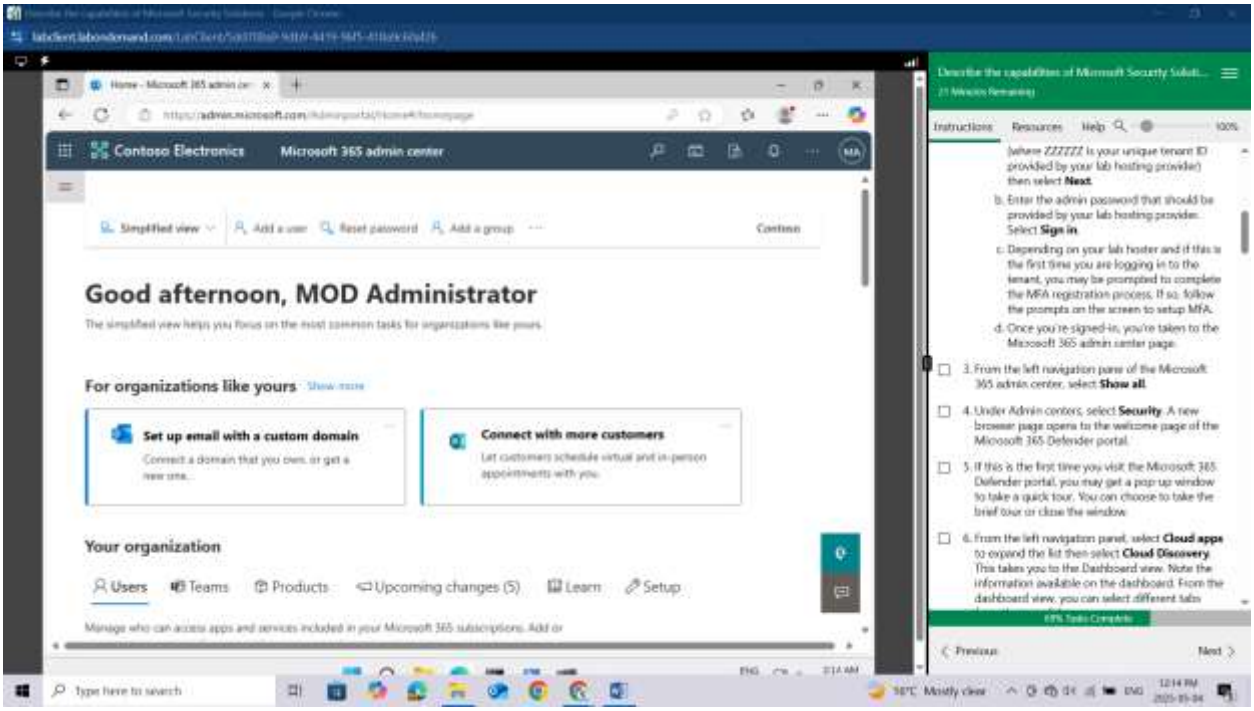


Enter the admin password that should be provided by your lab hosting provider. Select **Sign in.**

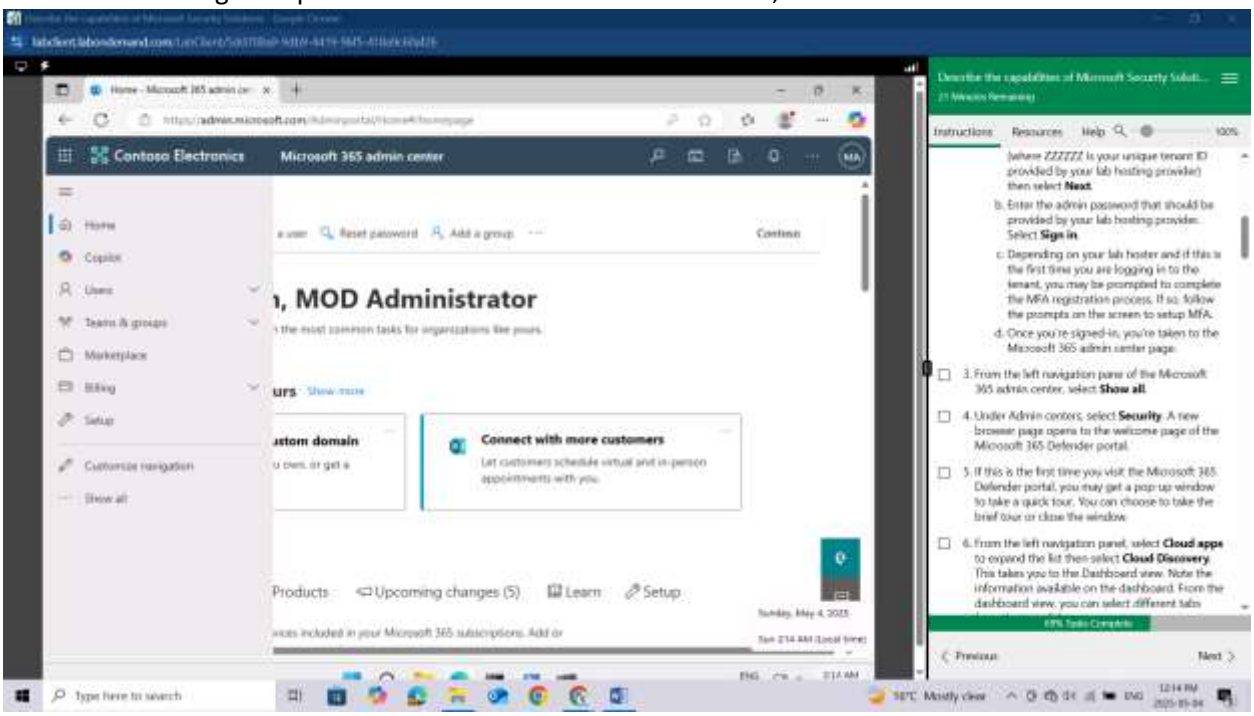


Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup **MFA**.

Once you're signed-in, you're taken to the Microsoft 365 admin center page.

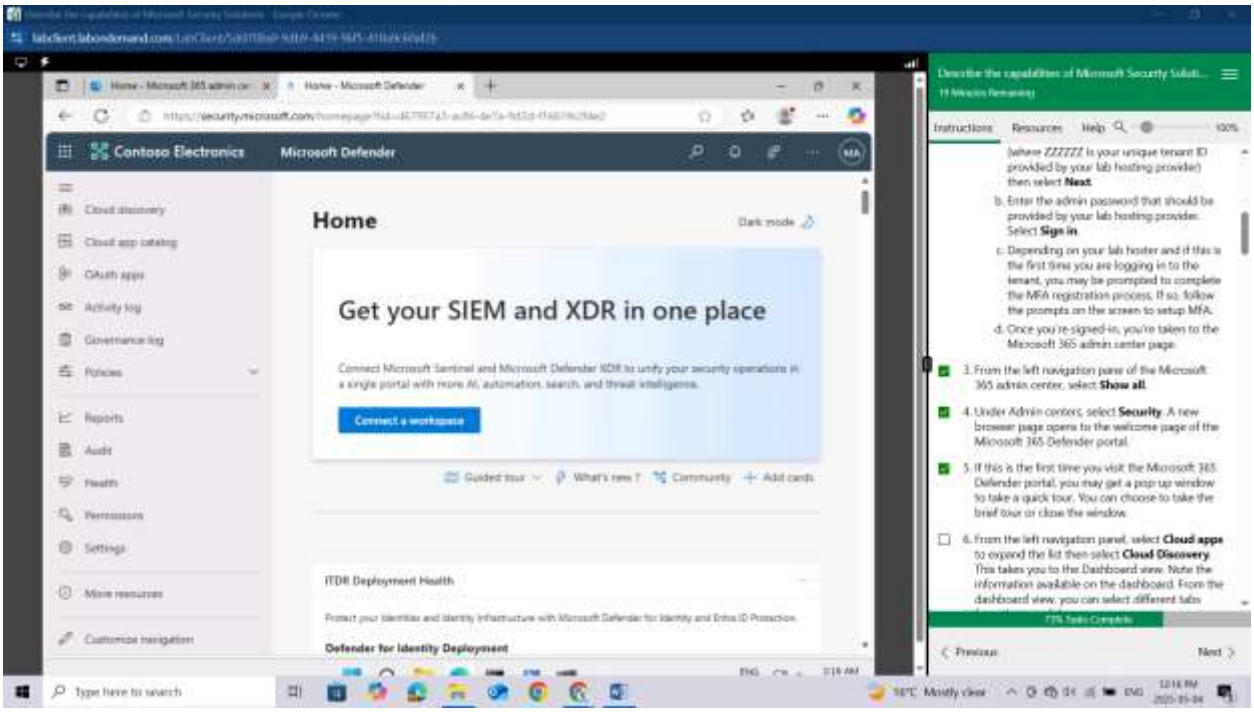


From the left navigation pane of the Microsoft 365 admin center, select **Show all.**



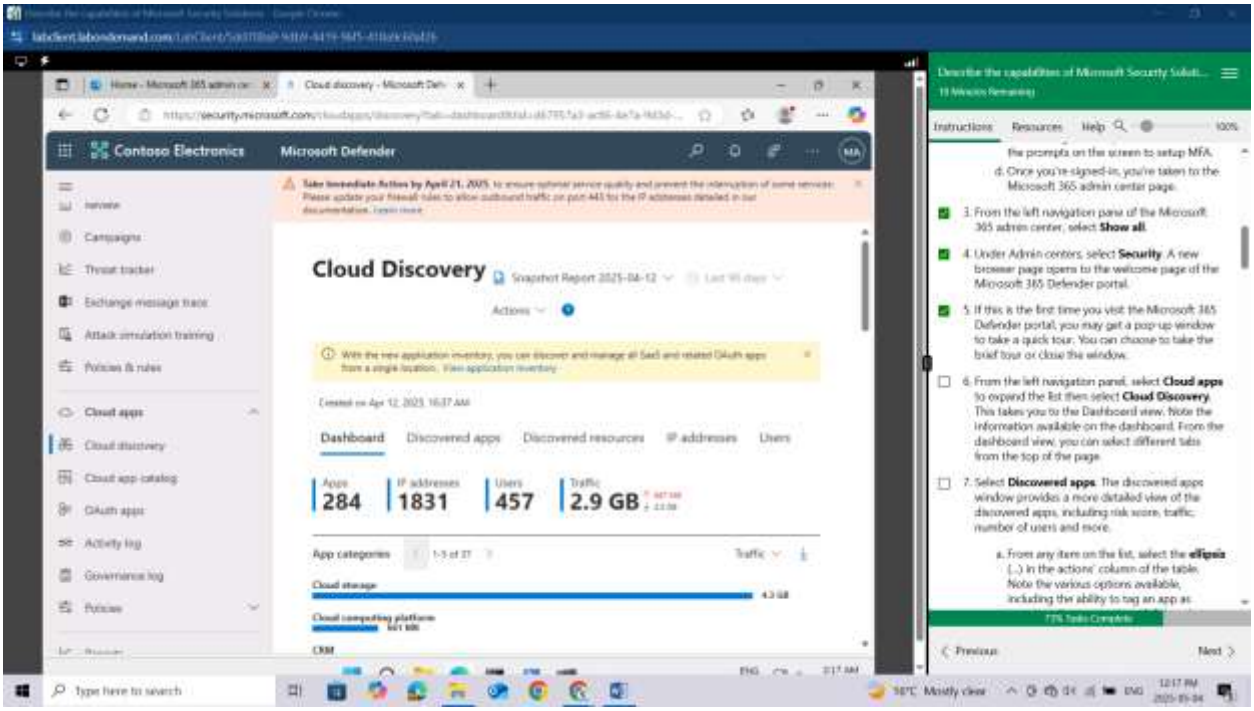
Under Admin centers, select **Security**. A new browser page opens to the welcome page of the Microsoft 365 Defender portal.

If this is the first time you visit the Microsoft 365 Defender portal, you may get a pop-up window to take a quick tour. You can choose to take the brief tour or close the window.



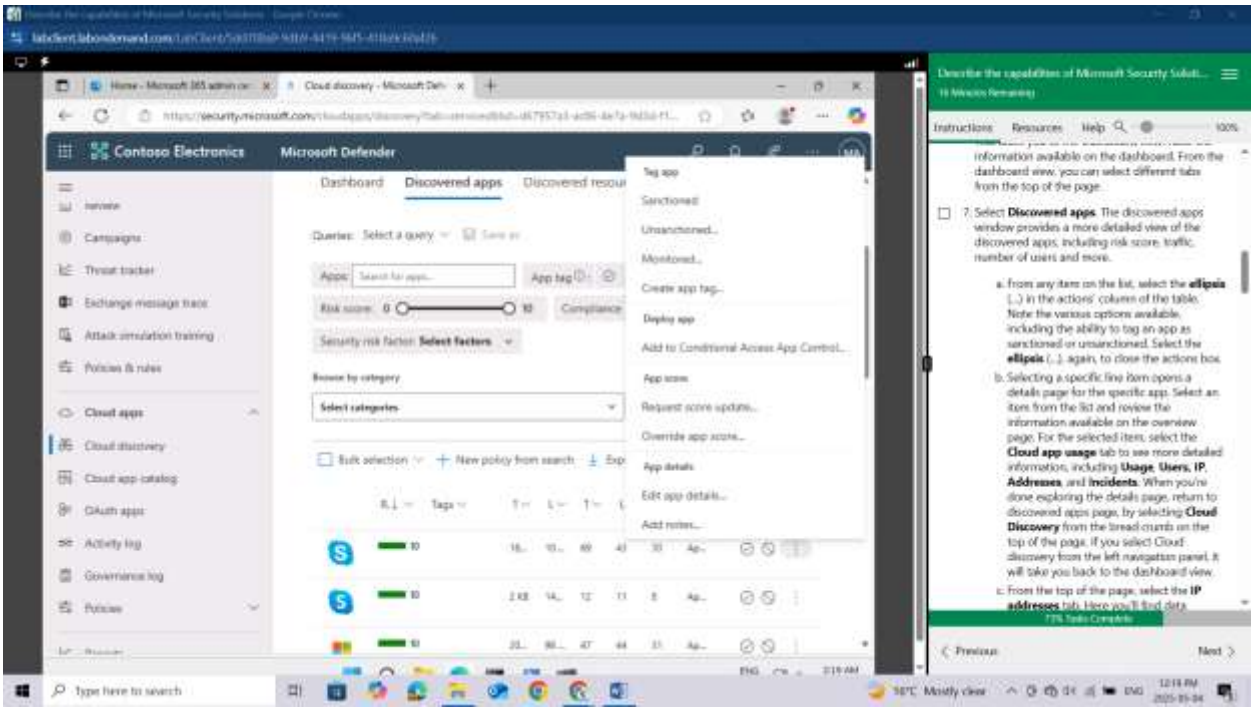
From the left navigation panel, select **Cloud apps** to expand the list then select **Cloud Discovery**. This

takes you to the Dashboard view. Note the information available on the dashboard. From the dashboard view, you can select different tabs from the top of the page.

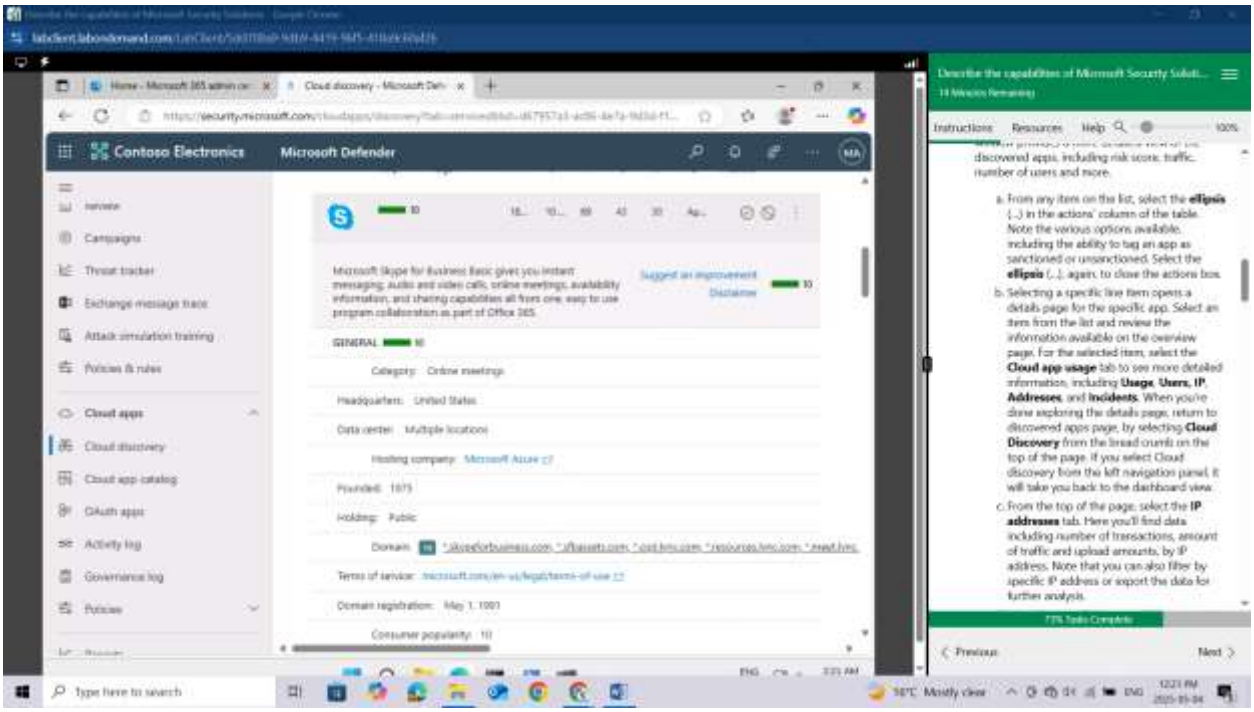


Select **Discovered apps.** The discovered apps window provides a more detailed view of the discovered apps, including risk score, traffic, number of users and more.

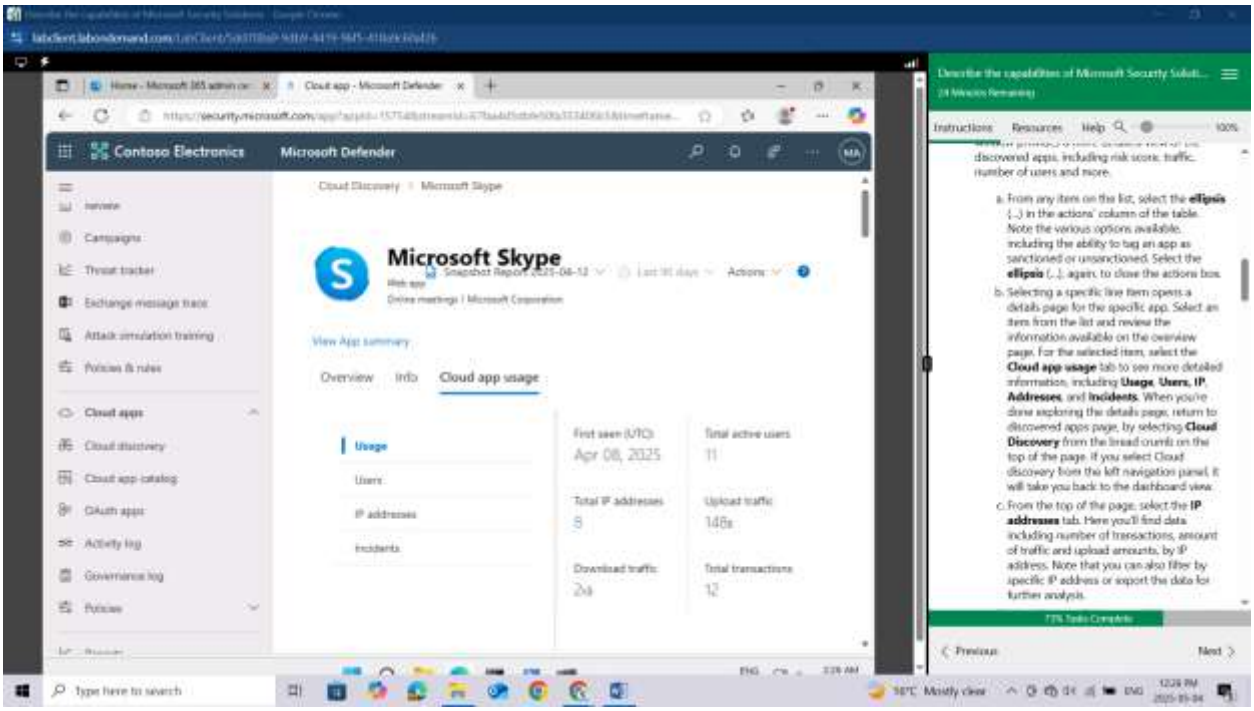
From any item on the list, select the ellipsis **(…)** in the actions' column of the table. Note the various options available, including the ability to tag an app as sanctioned or unsanctioned. Select the ellipsis **(…),** again, to close the actions box.



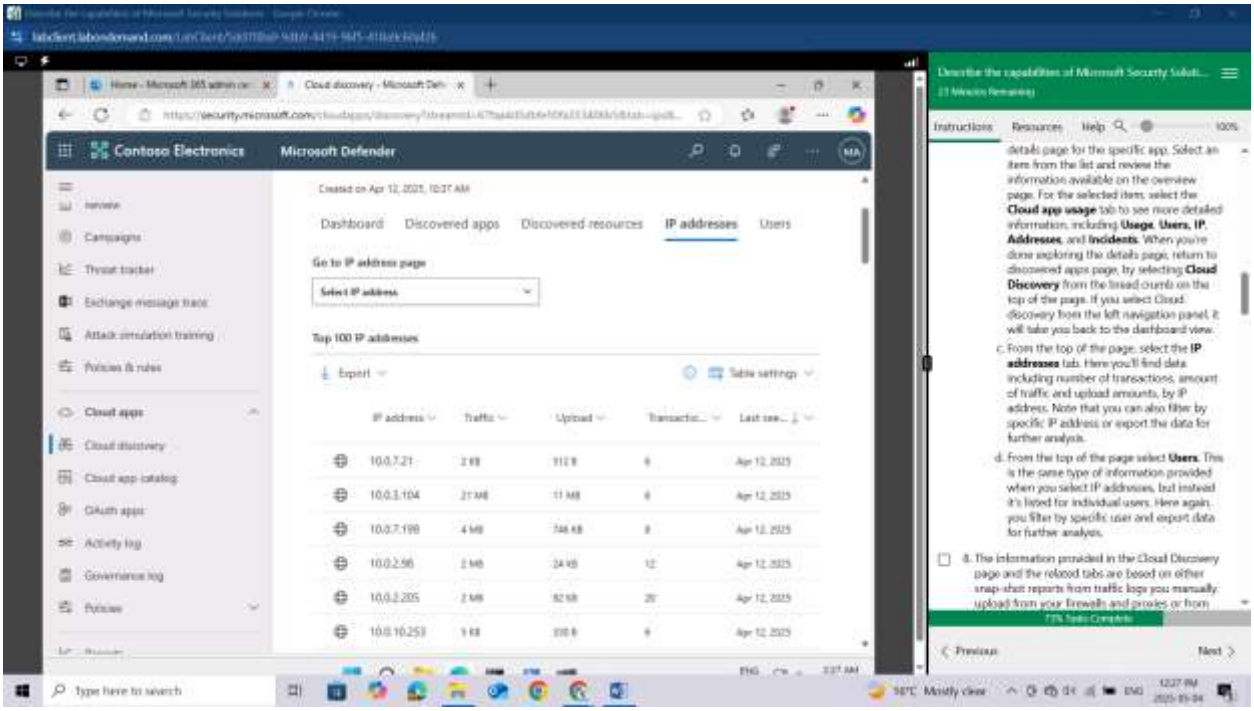
Selecting a specific line item opens a details page for the specific app. Select an item from the list and review the information available on the overview page.



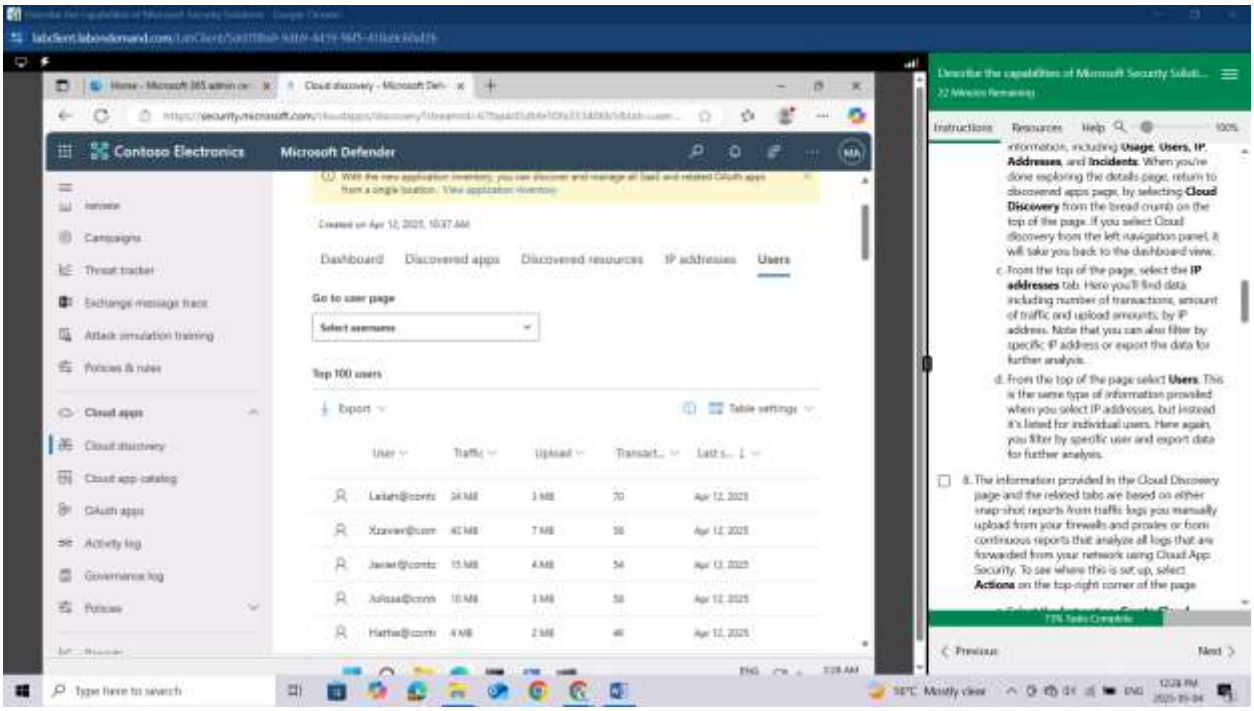
For the selected item, select the **Cloud app usage** tab to see more detailed information, including **Usage, Users, IP, Addresses, and Incidents**. When you're done exploring the details page, return to discovered apps page, by selecting Cloud Discovery from the bread crumb on the top of the page. If you select Cloud discovery from the left navigation panel, it will take you back to the dashboard view.



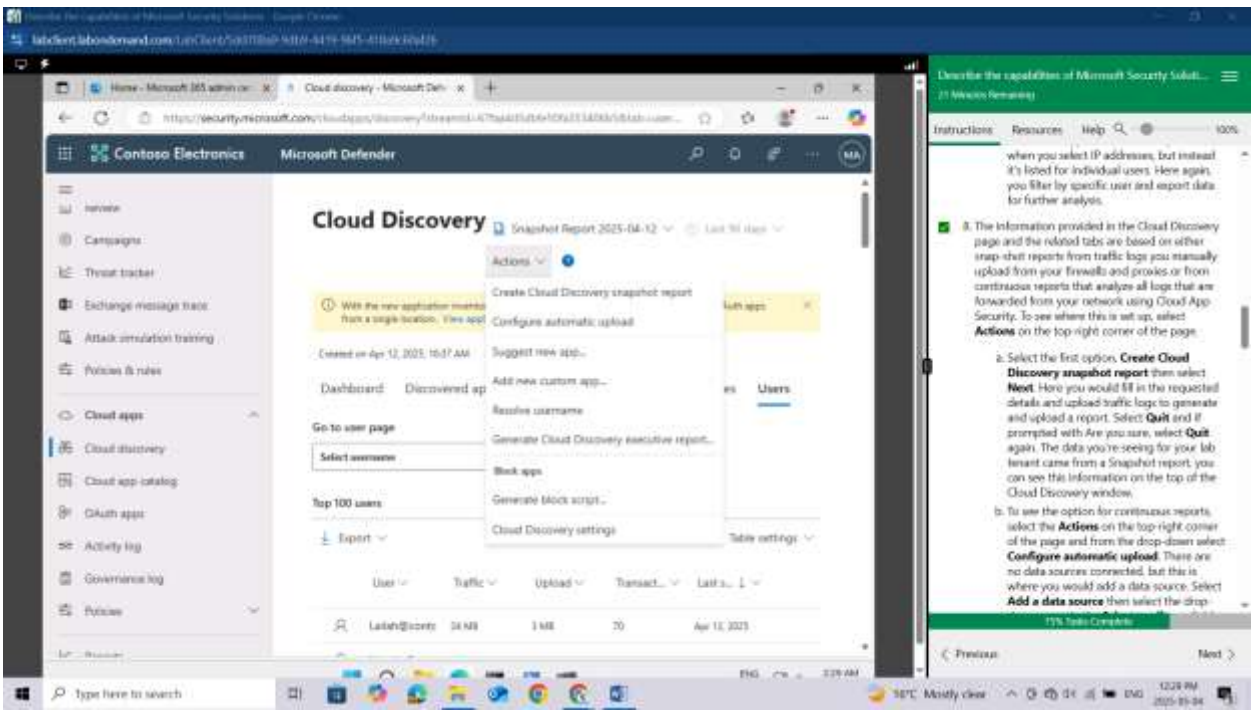
From the top of the page, select the **IP addresses tab**. Here you'll find data including number of transactions, amount of traffic and upload amounts, by IP address. Note that you can also filter by specific IP address or export the data for further analysis.



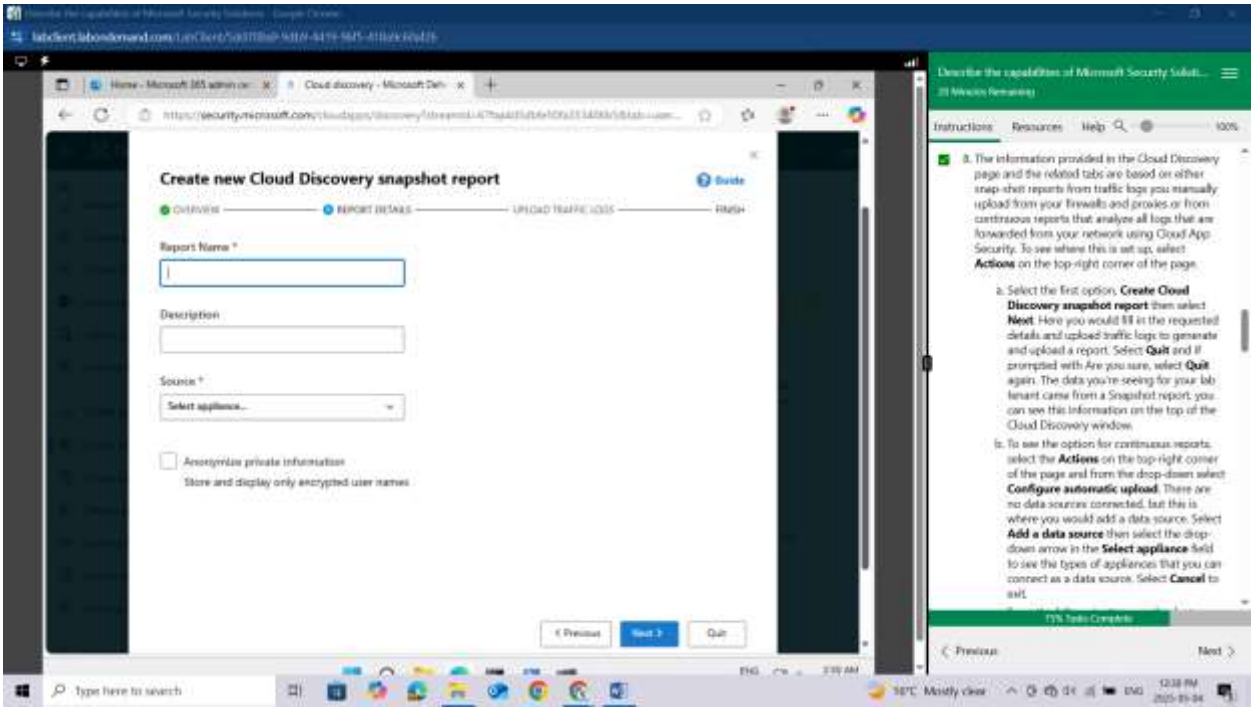
From the top of the page select **Users**. This is the same type of information provided when you select IP addresses, but instead it's listed for individual users. Here again, you filter by specific user and export data for further analysis.



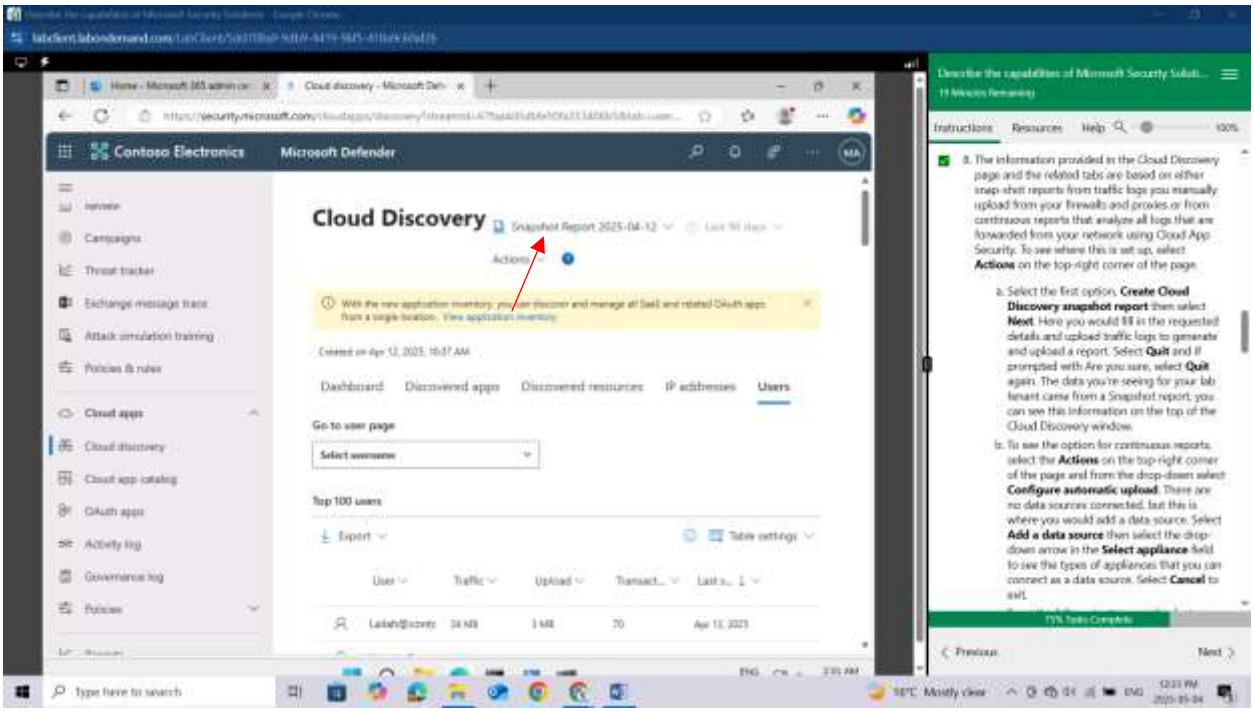
The information provided in the Cloud Discovery page and the related tabs are based on either snap-shot reports from traffic logs you manually upload from your firewalls and proxies or from continuous reports that analyze all logs that are forwarded from your network using Cloud App Security. To see where this is set up, select **Actions** on the top-right corner of the page.



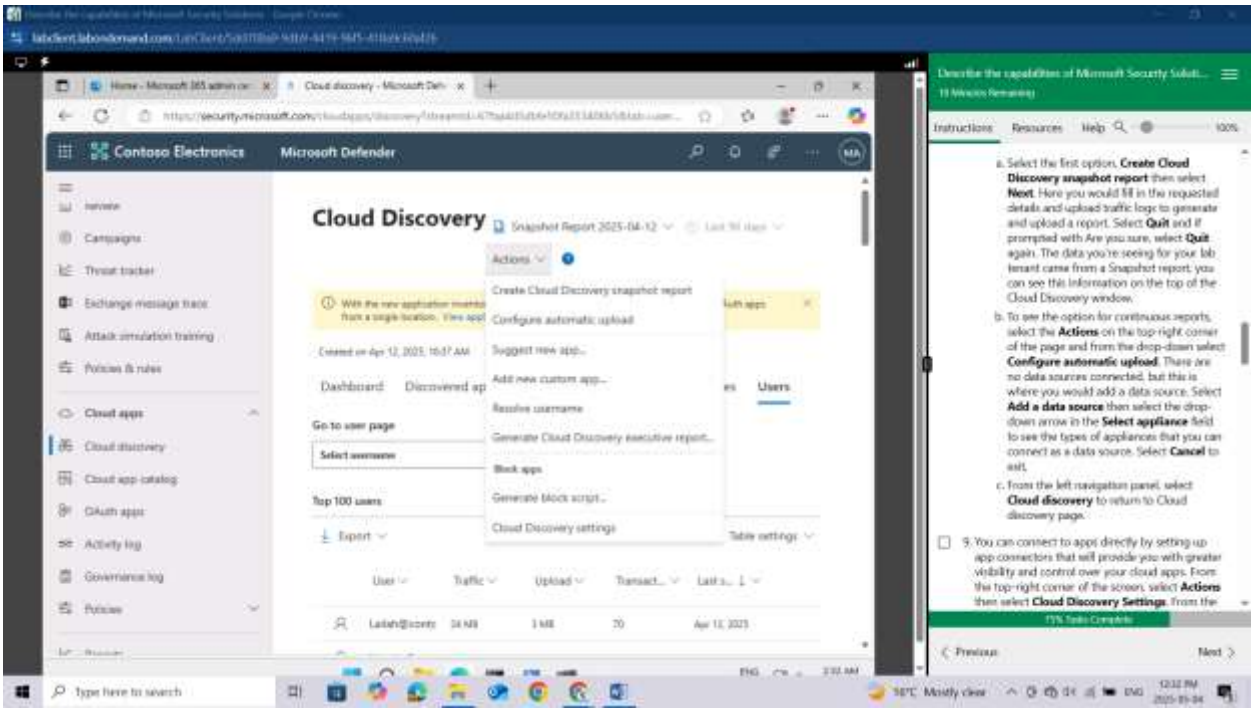
Select the first option, **Create Cloud Discovery snapshot report** then select **Next**. Here you would fill in the requested details and upload traffic logs to generate and upload a report. Select **Quit** and if prompted with **Are you sure**, select **Quit** again.



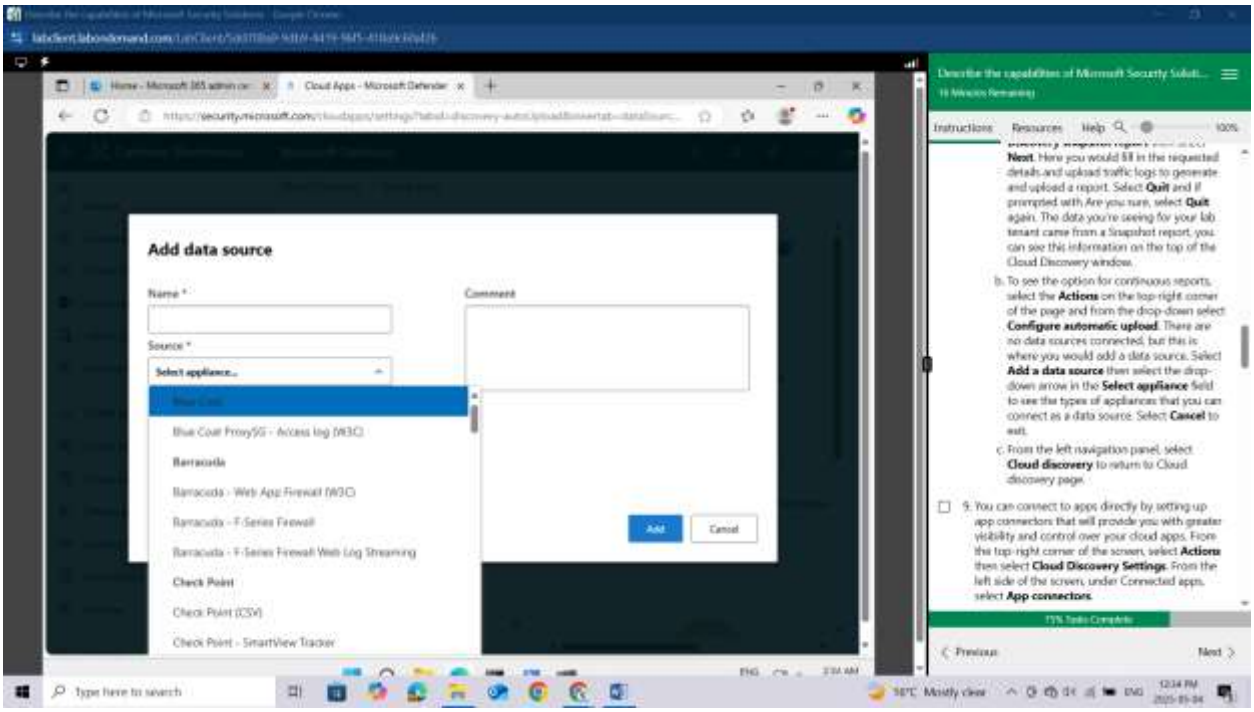
The data you're seeing for your lab tenant came from a Snapshot report, you can see this information on the top of the Cloud Discovery window.



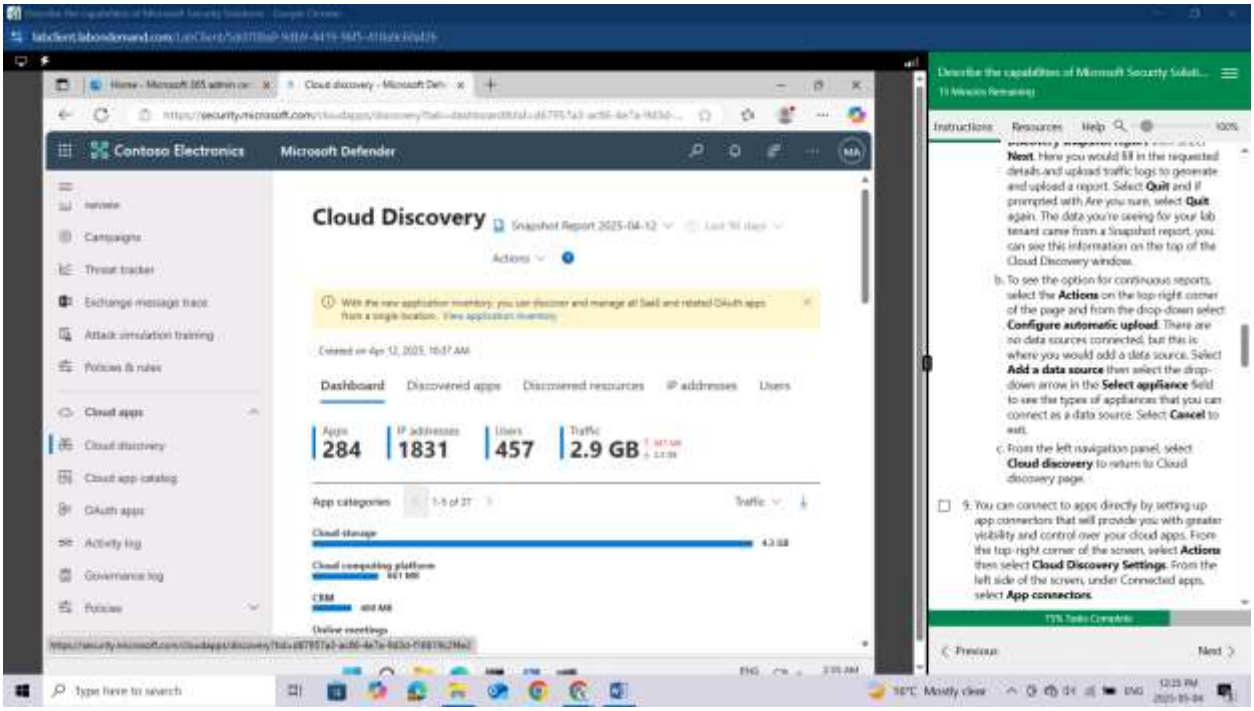
To see the option for continuous reports, select the **Actions** on the top-right corner of the page and from the drop-down select **Configure automatic upload**.



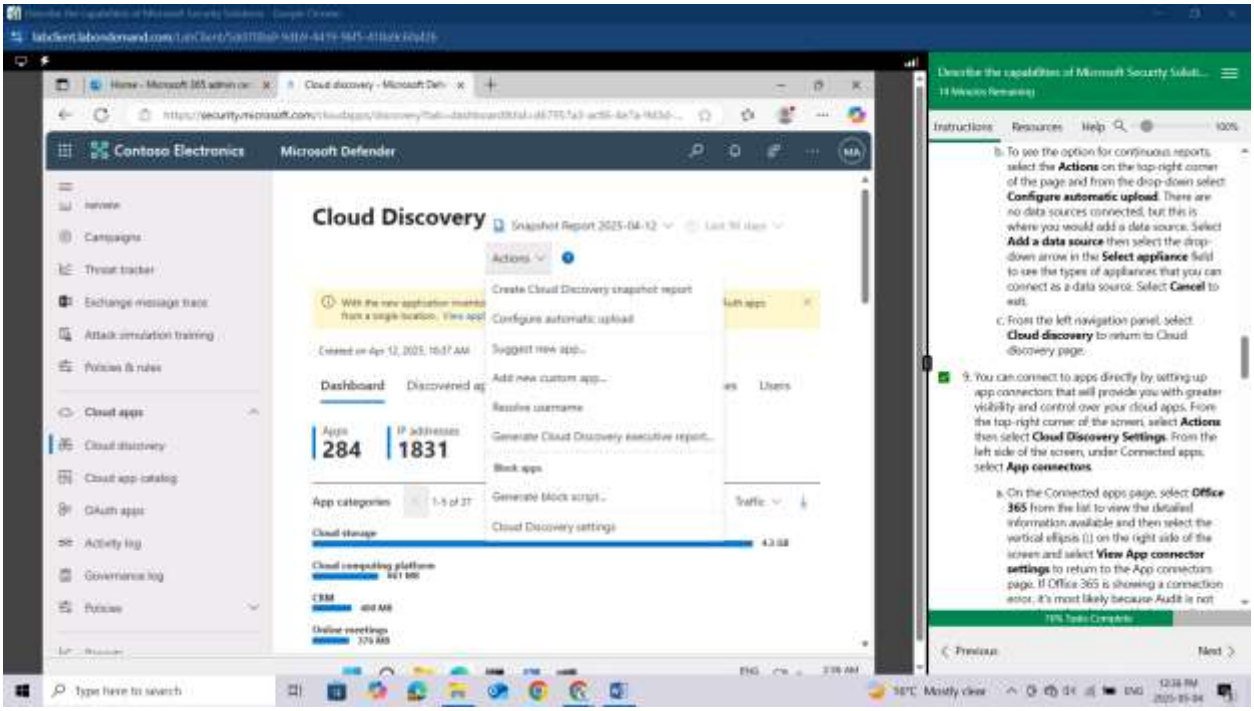
There are no data sources connected, but this is where you would add a data source. Select **Add a data source** then select the drop-down arrow in the Select **appliance** field to see the types of appliances that you can connect as a data source. Select **Cancel** to exit,



From the left navigation panel, select **Cloud discovery** to return to Cloud discovery page.

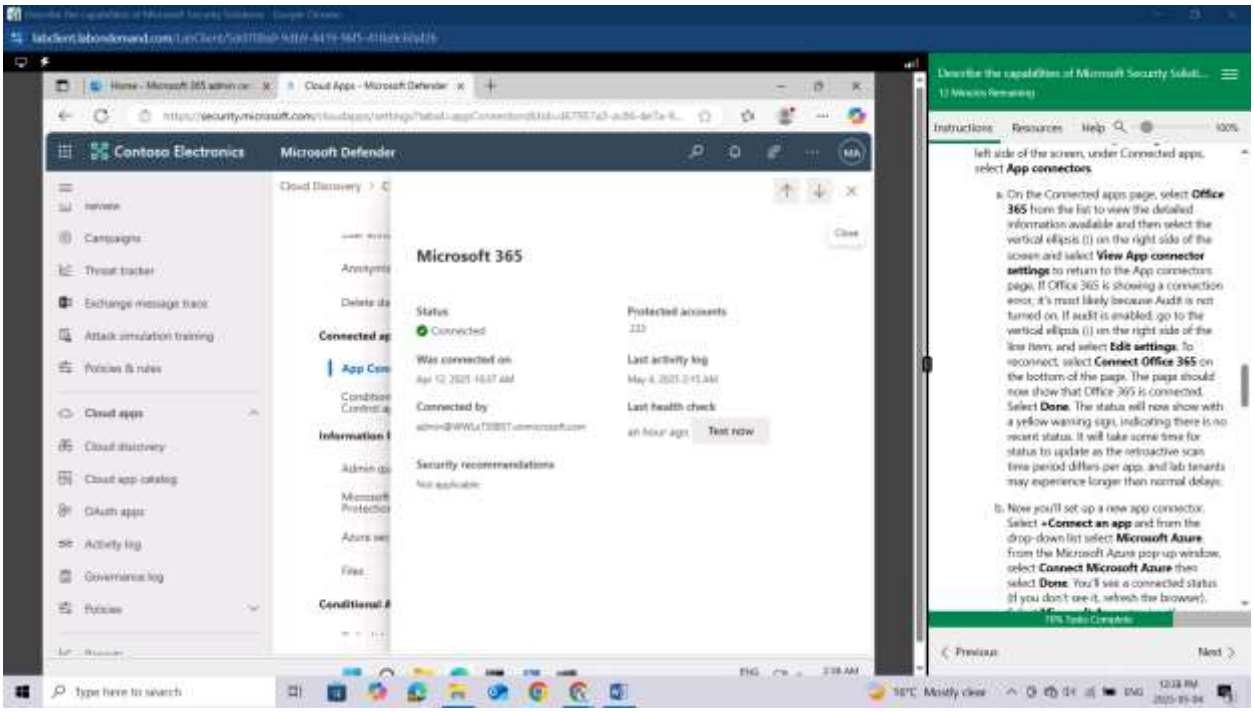


You can connect to apps directly by setting up app connectors that will provide you with greater visibility and control over your cloud apps. From the top-right corner of the screen, select **Actions** then select **Cloud Discovery Settings**.

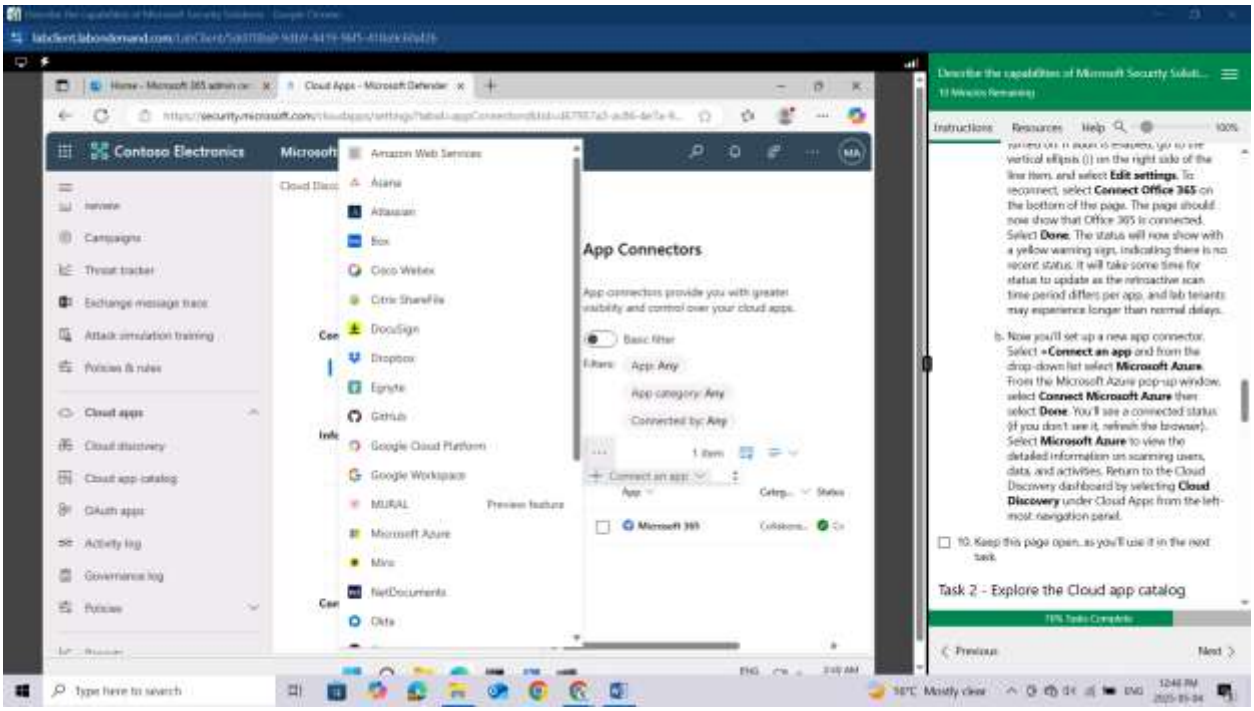


From the left side of the screen, under Connected apps, select **App connectors**.

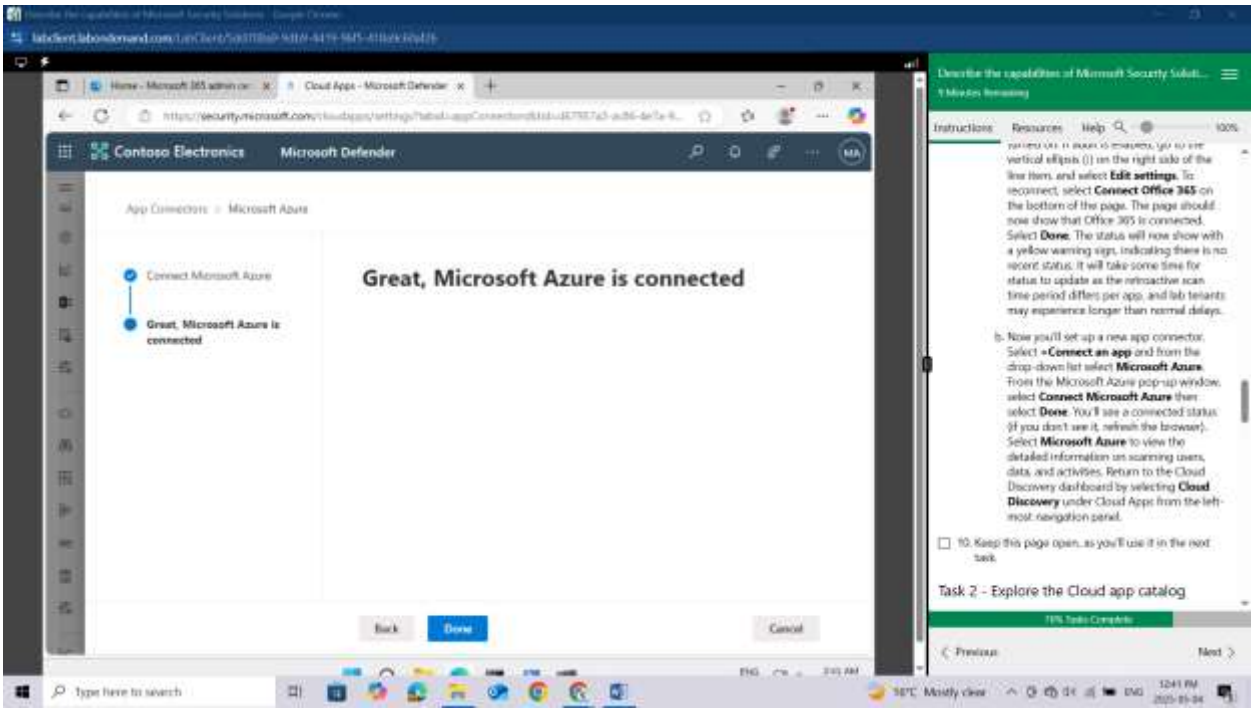
On the Connected apps page, select **Office 365** from the list to view the detailed information available and then select the vertical ellipsis (⋮) on the right side of the screen and select View App connector settings to return to the App connectors page. If Office 365 is showing a connection error, it's most likely because Audit is not turned on. If audit is enabled, go to the vertical ellipsis (⋮) on the right side of the line item, and select Edit settings. To reconnect, select Connect Office 365 on the bottom of the page. The page should now show that Office 365 is connected. Select Done. The status will now show with a yellow warning sign, indicating there is no recent status. It will take some time for status to update as the retroactive scan time period differs per app, and lab tenants may experience longer than normal delays.



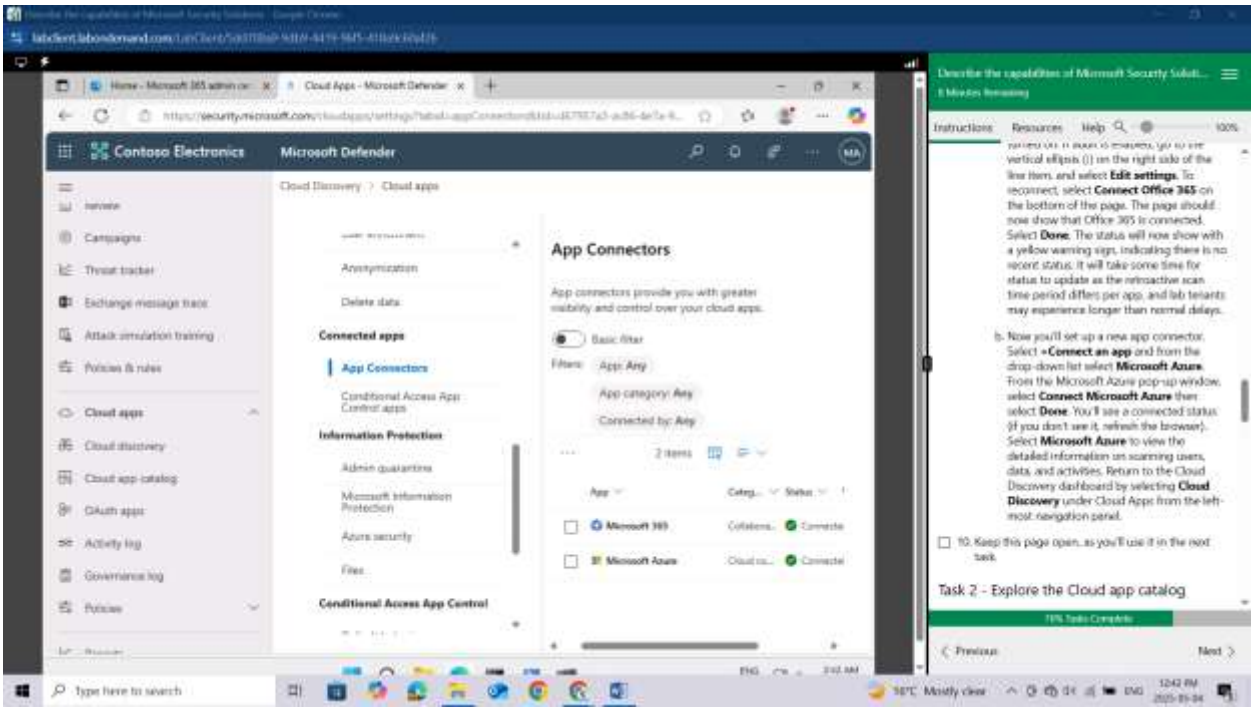
Now you'll set up a new app connector. Select **+Connect an app** and from the drop-down list select **Microsoft Azure.**



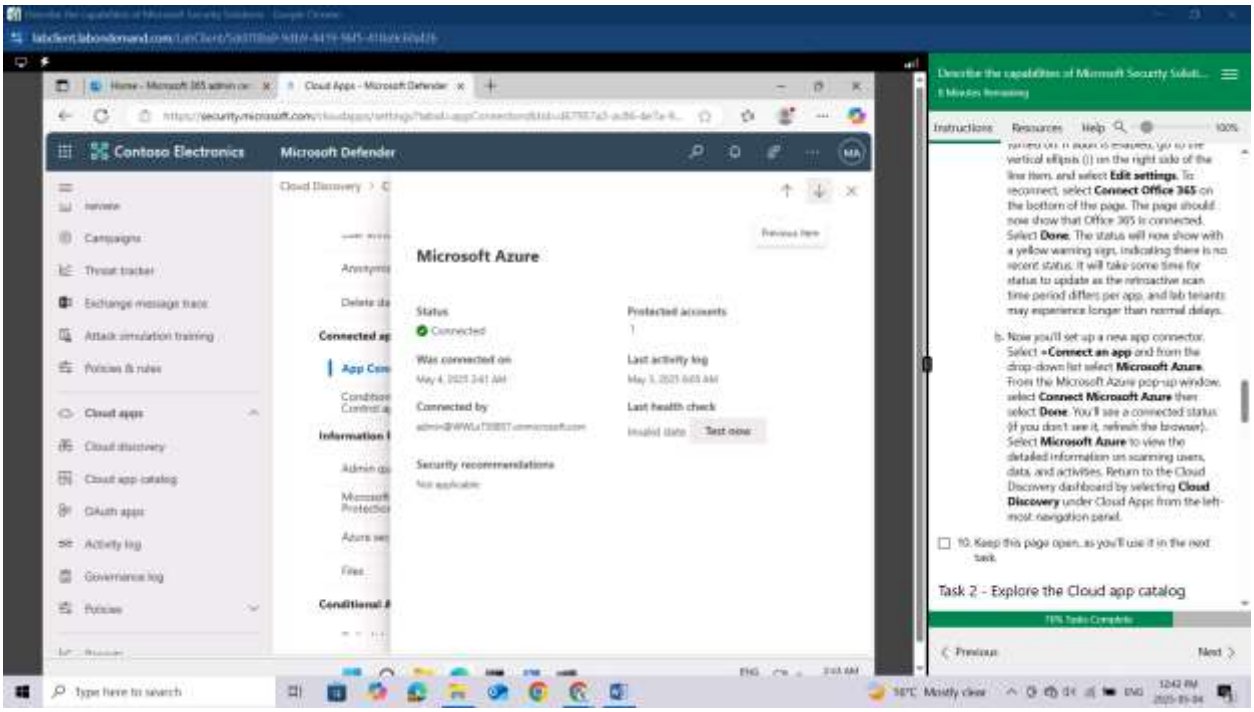
From the Microsoft Azure pop-up window, select **Connect Microsoft Azure** then select **Done**.



You'll see a connected status (if you don't see it, refresh the browser).

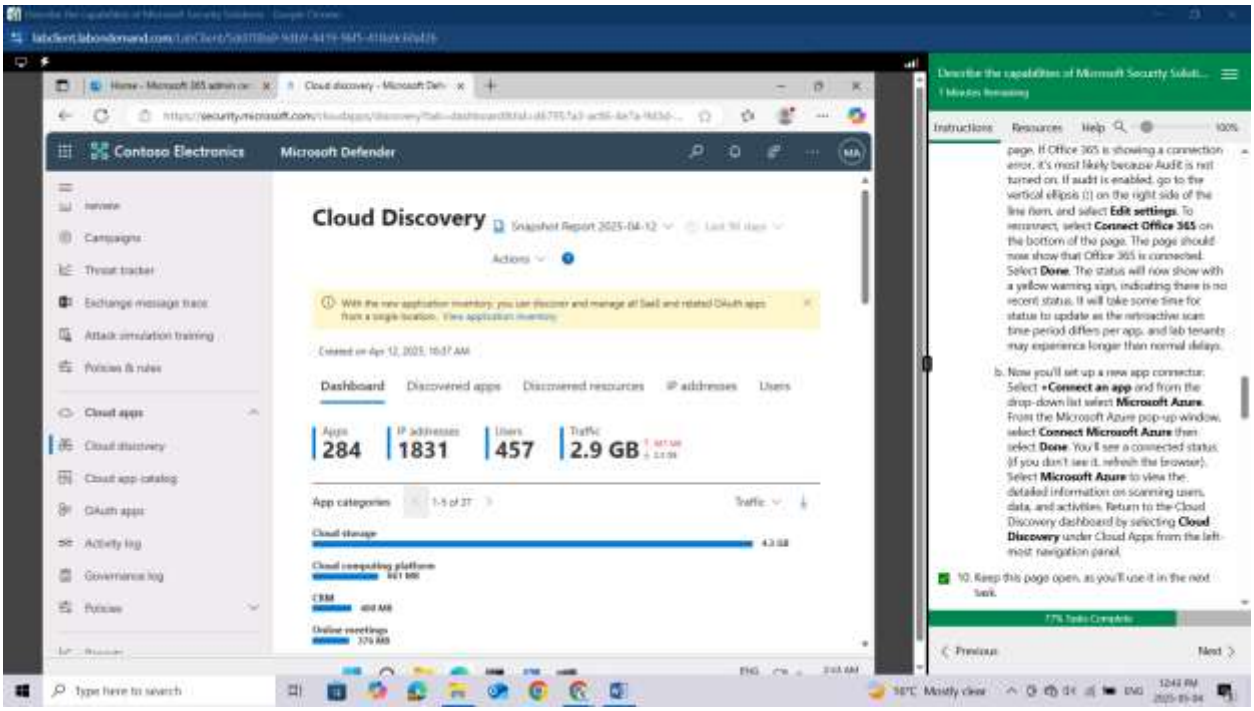


Select **Microsoft Azure** to view the detailed information on scanning users, data, and activities.



Return to the Cloud Discovery dashboard by selecting **Cloud Discovery** under Cloud Apps from the left-most navigation panel.

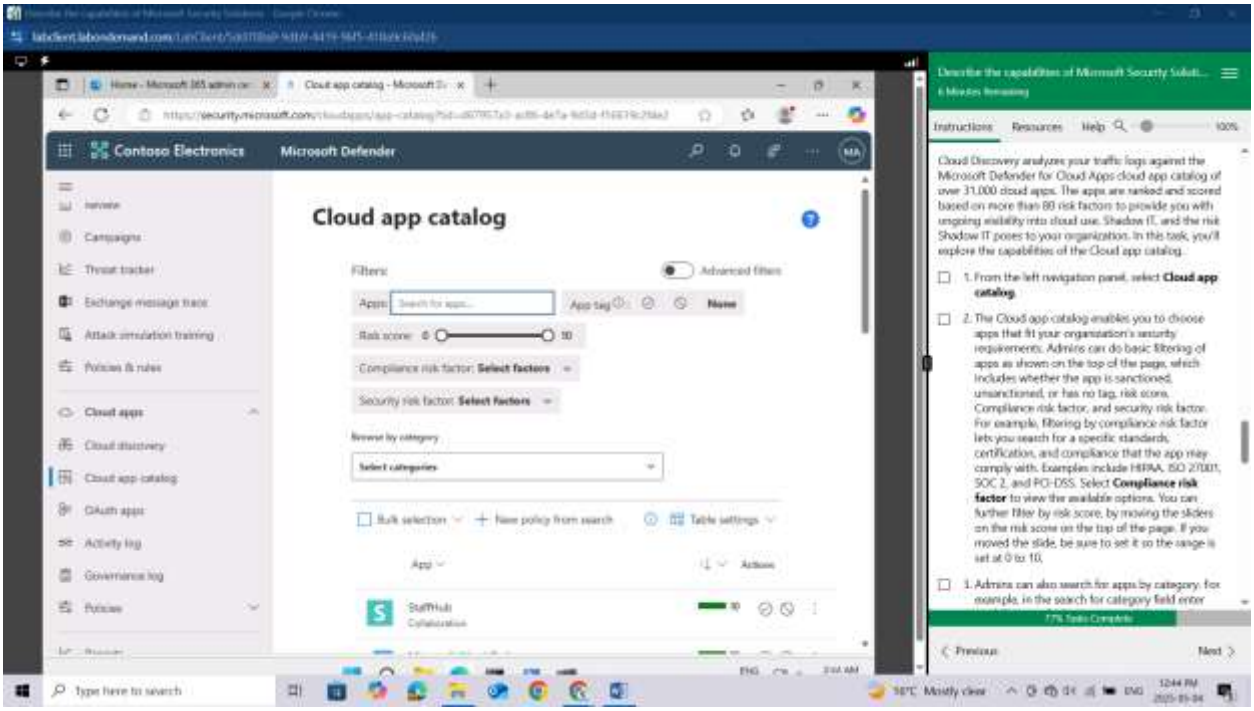
Keep this page open, as you'll use it in the next task.



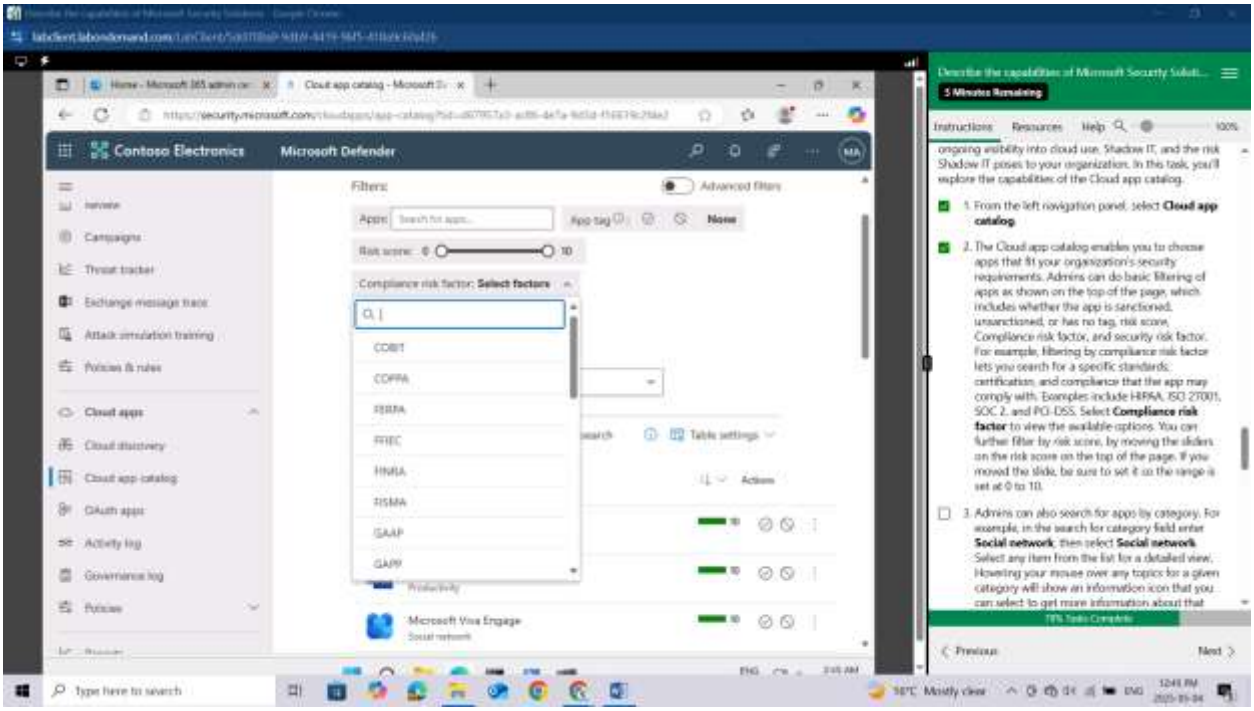
Task 2 - Explore the Cloud app catalog

Cloud Discovery analyzes your traffic logs against the Microsoft Defender for Cloud Apps cloud app catalog of over 31,000 cloud apps. The apps are ranked and scored based on more than 80 risk factors to provide you with ongoing visibility into cloud use, Shadow IT, and the risk Shadow IT poses to your organization. In this task, you'll explore the capabilities of the Cloud app catalog.

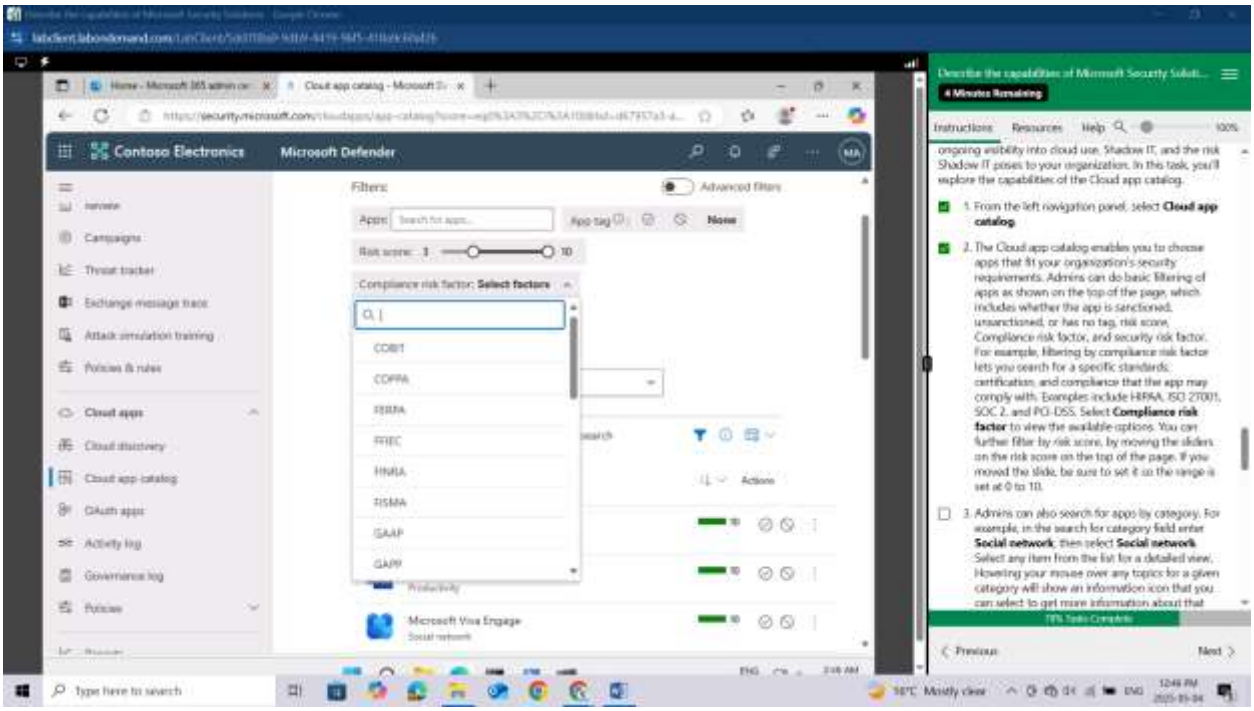
From the left navigation panel, select **Cloud app catalog**.



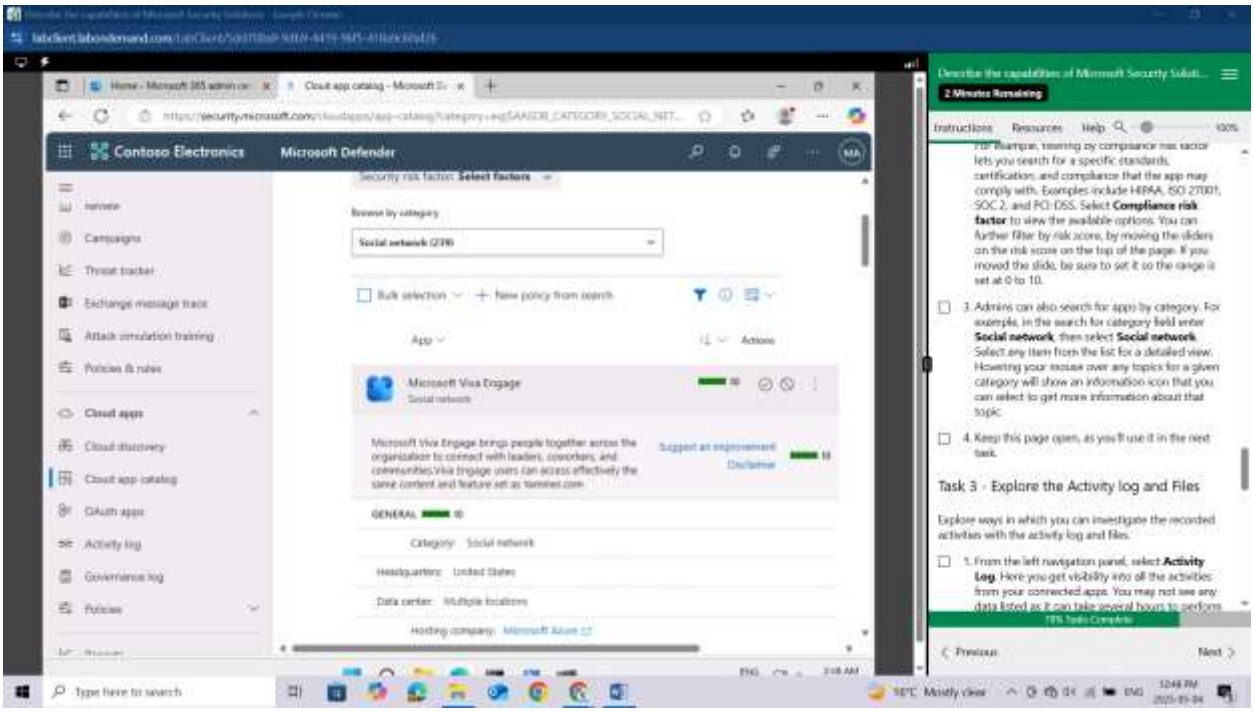
The Cloud app catalog enables you to choose apps that fit your organization's security requirements. Admins can do basic filtering of apps as shown on the top of the page, which includes whether the app is sanctioned, unsanctioned, or has no tag, risk score, Compliance risk factor, and security risk factor. For example, filtering by compliance risk factor lets you search for a specific standards, certification, and compliance that the app may comply with. Examples include HIPAA, ISO 27001, SOC 2, and PCI-DSS. Select **Compliance risk factor** to view the available options.



You can further filter by risk score, by moving the sliders on the risk score on the top of the page. If you moved the slide, be sure to set it so the range is set at 0 to 10.



Admins can also search for apps by category. For example, in the search for category field enter **Social network**, then select **Social network**. Select any item from the list for a detailed view. Hovering your mouse over any topics for a given category will show an information icon that you can select to get more information about that topic.

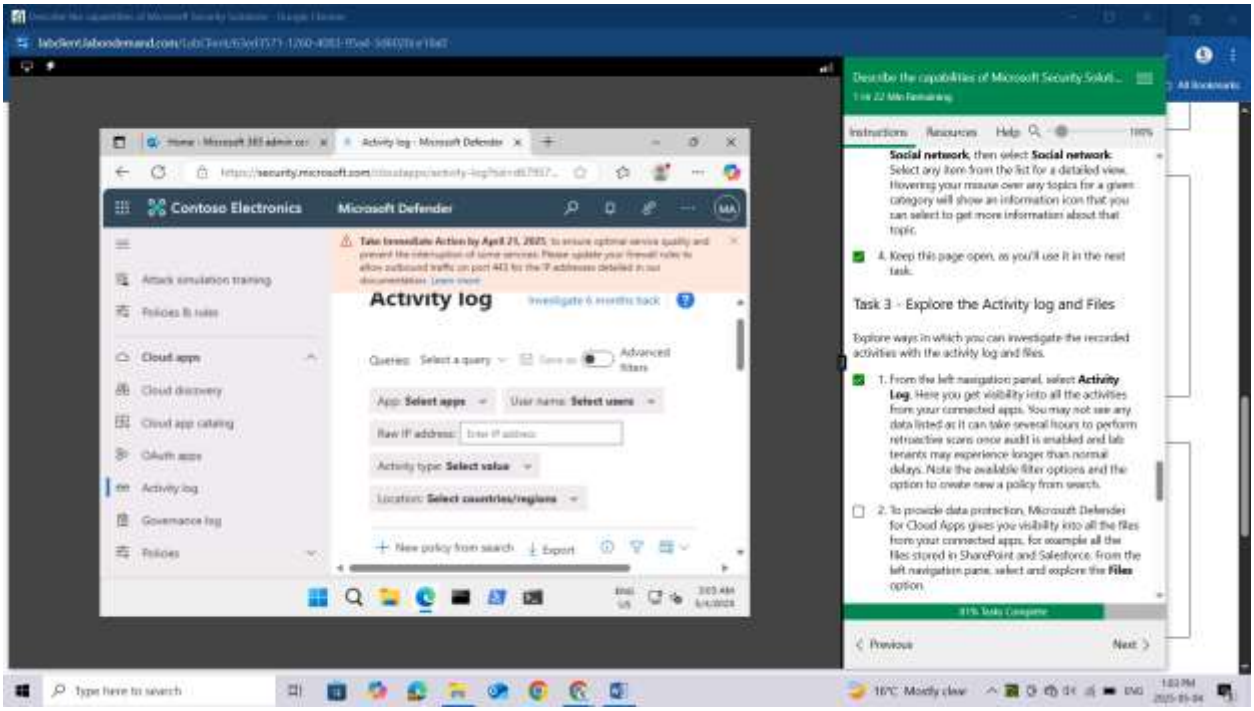


Keep this page open, as you'll use it in the next task.

Task 3 - Explore the Activity log and Files

Explore ways in which you can investigate the recorded activities with the activity log and files.

From the left navigation panel, select **Activity Log**. Here you get visibility into all the activities from your connected apps. You may not see any data listed as it can take several hours to perform retroactive scans once audit is enabled and lab tenants may experience longer than normal delays. Note the available filter options and the option to create new a policy from search.

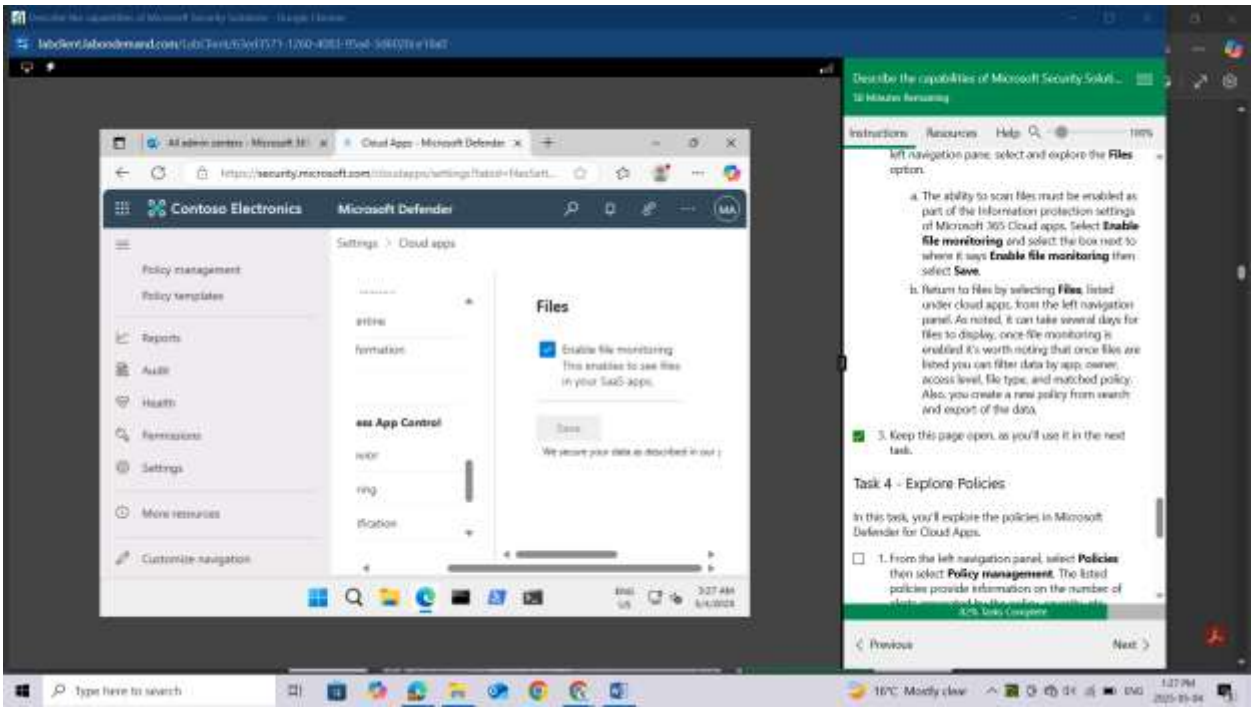


To provide data protection, Microsoft Defender for Cloud Apps gives you visibility into all the files from your connected apps, for example all the files stored in SharePoint and Salesforce. From the left navigation pane, select and **explore the Files option.**

The ability to scan files must be enabled as part of the Information protection settings of Microsoft 365 Cloud apps. Select **Enable file monitoring** and select the box next to where it says **Enable file monitoring** then select **Save**.

Return to files by selecting **Files**, listed under cloud apps, from the left navigation panel. As noted, it can take several days for files to display, once file monitoring is enabled it's worth noting that once files are listed you can filter data by app, owner, access level, file type, and matched policy. Also, you create a new policy from search and export of the data.

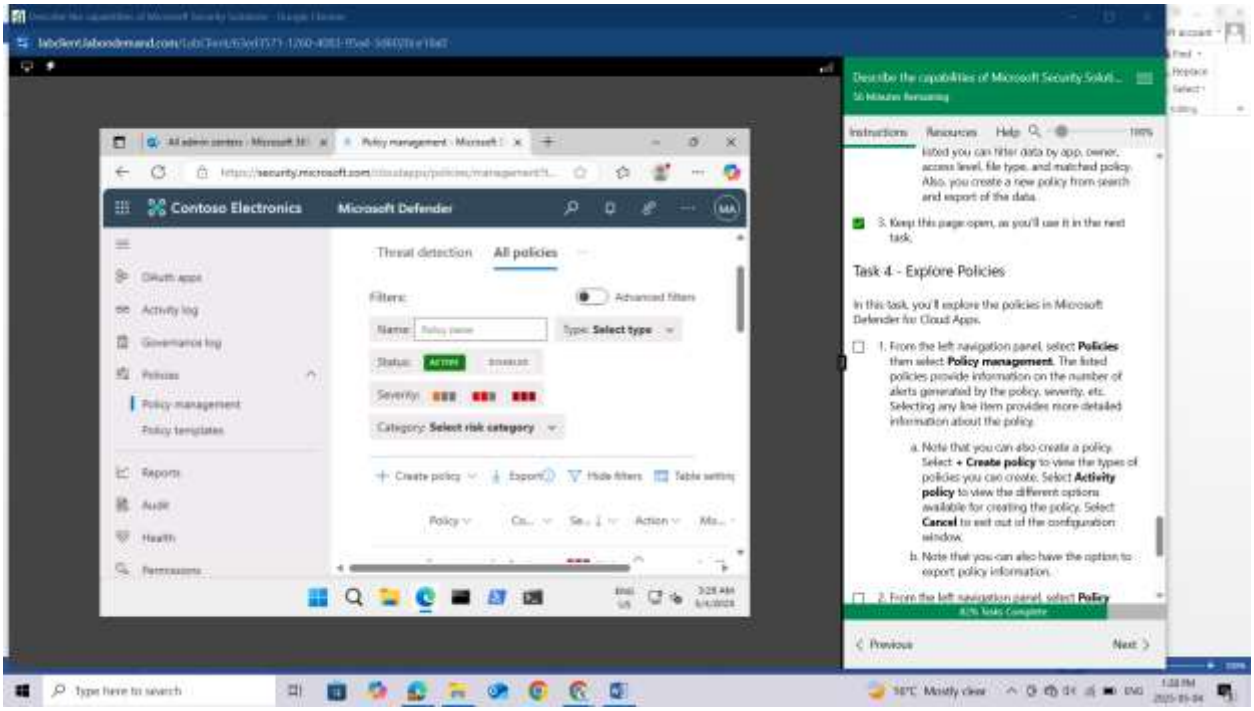
Keep this page open, as you'll use it in the next task.



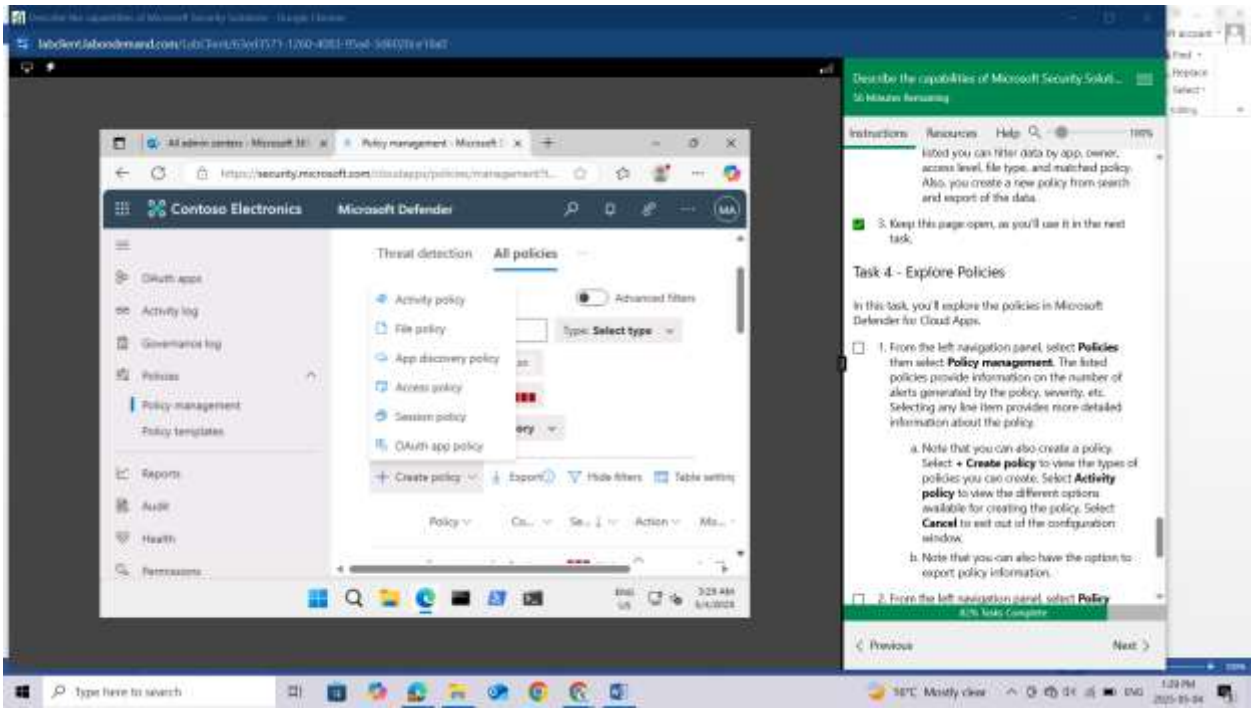
Task 4 - Explore Policies

In this task, you'll explore the policies in Microsoft Defender for Cloud Apps.

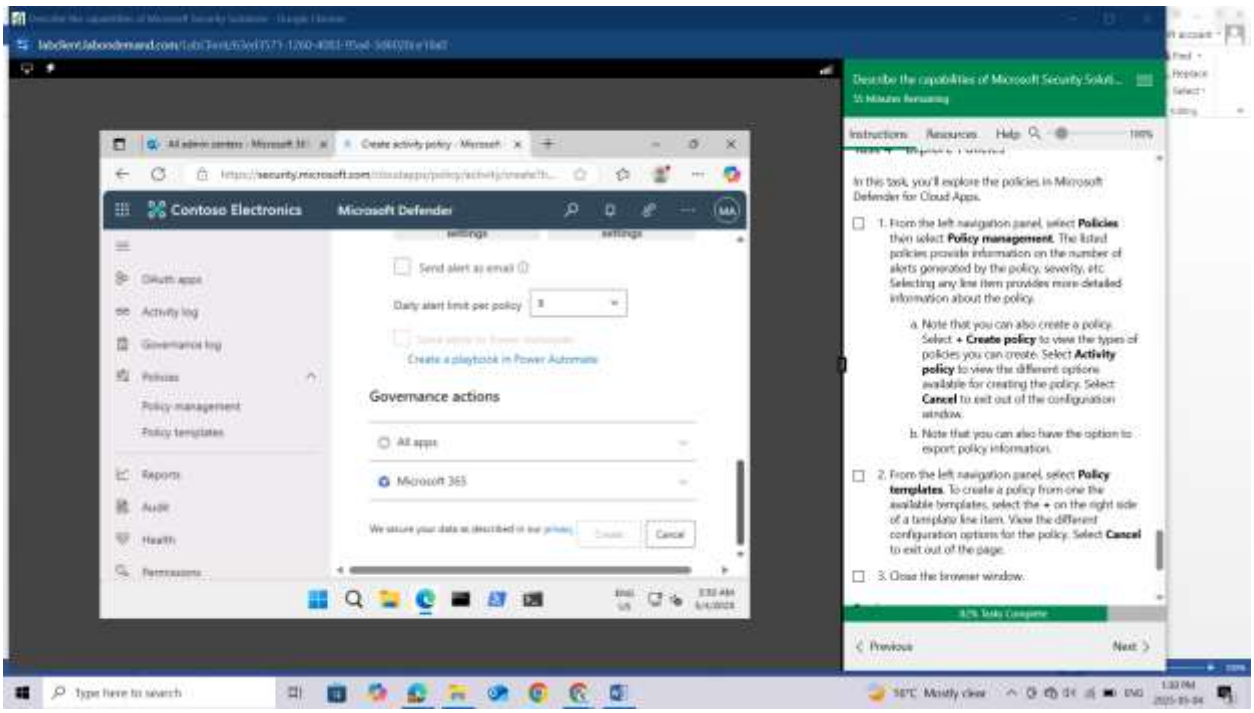
From the left navigation panel, select **Policies** then select **Policy management**. The listed policies provide information on the number of alerts generated by the policy, severity, etc. Selecting any line item provides more detailed information about the policy.



Note that you can also create a policy. Select **+ Create policy** to view the types of policies you can create. Select **Activity policy** to view the different options available for creating the policy.

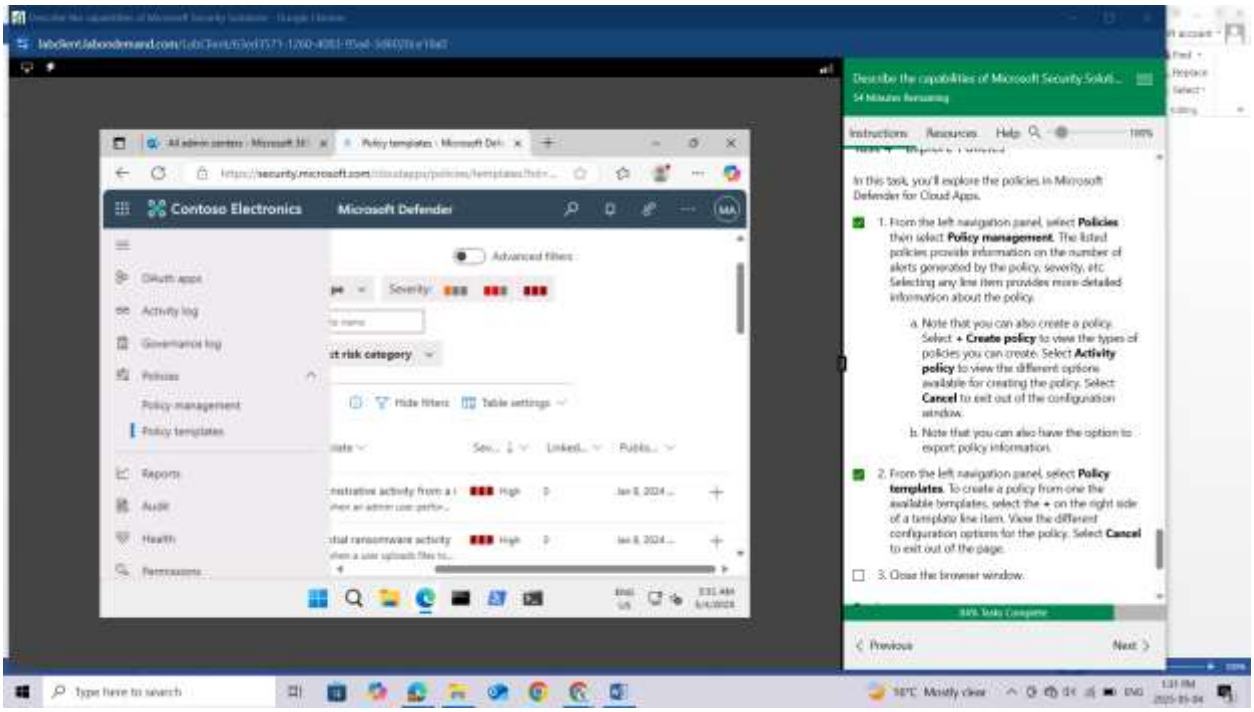


Select **Cancel** to exit out of the configuration window.

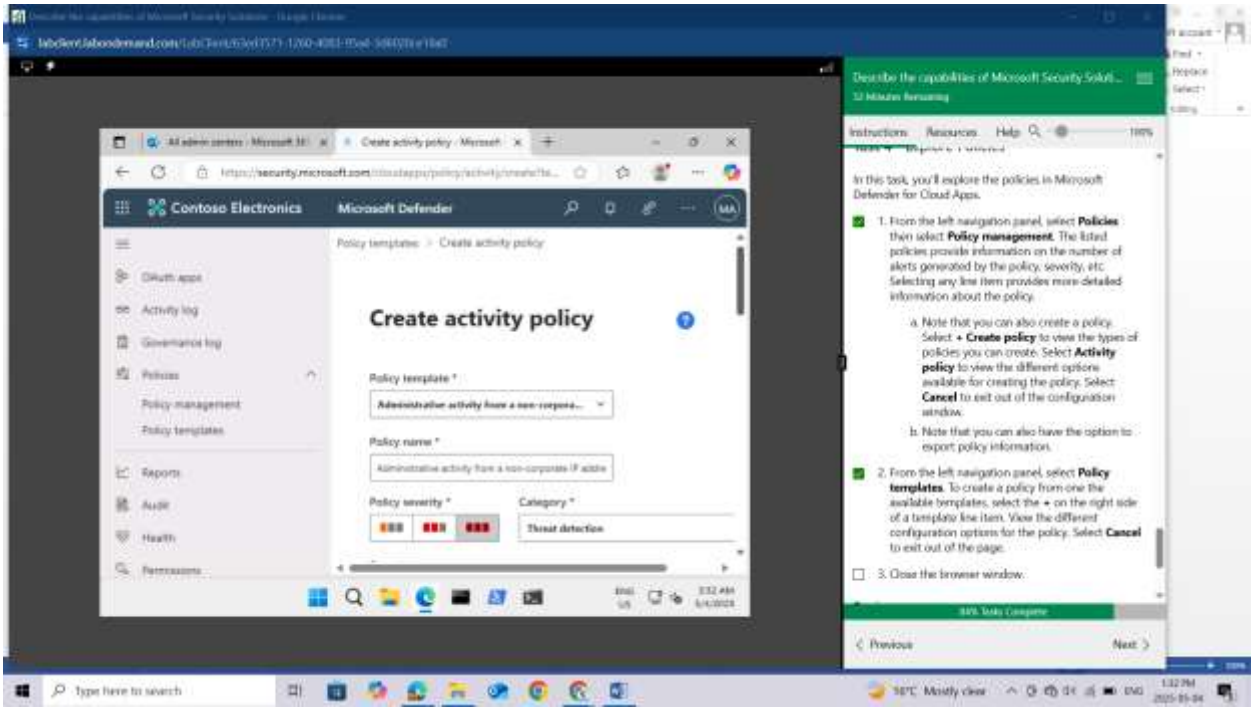


Note that you can also have the option to export policy information.

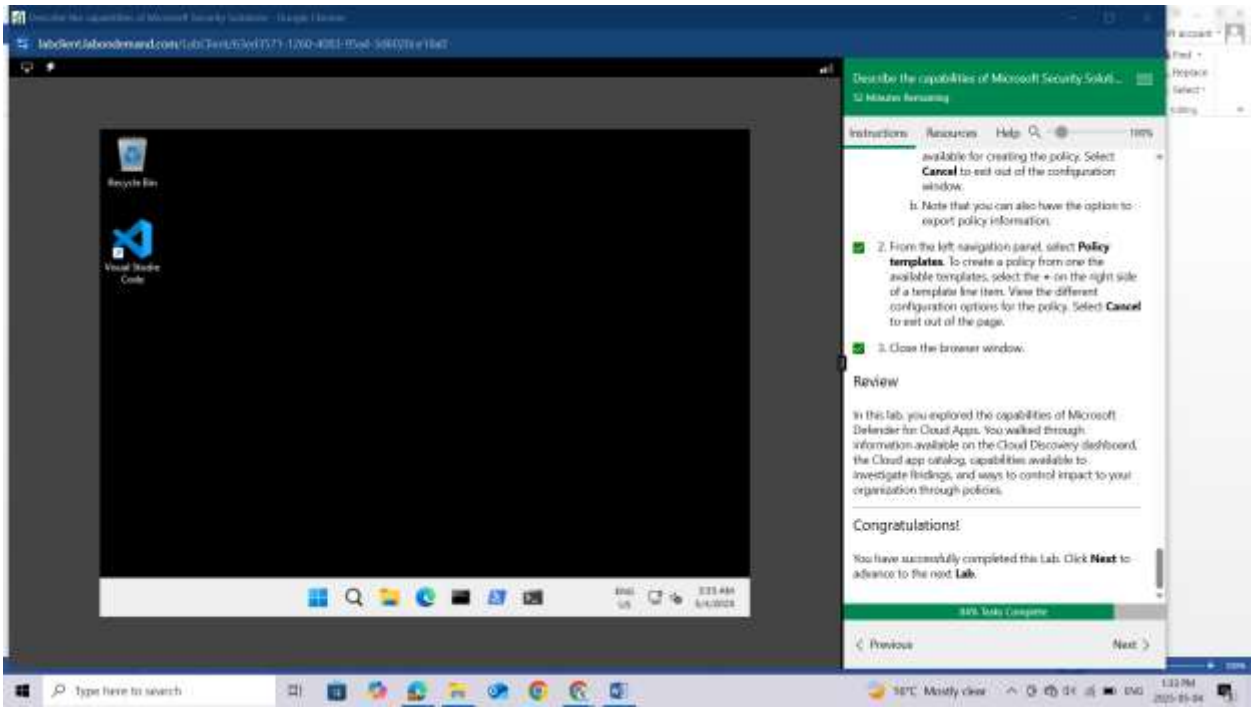
From the left navigation panel, select **Policy templates**. To create a policy from one the available templates, select the **+** on the right side of a template line item.



View the different configuration options for the policy. Select **Cancel** to exit out of the page.



Close the browser window.



Review

In this lab, you explored the capabilities of Microsoft Defender for Cloud Apps. You walked through information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies.

LAB: EXPLORE THE MICROSOFT DEFENDER PORTAL

This lab maps to the following Learn content:

Learning Path: Describe the capabilities of Microsoft security solutions

Module: Describe the threat protection capabilities of Microsoft Defender XDR

Unit: Describe the Microsoft Defender portal

Lab scenario

In this lab, you'll explore the Microsoft Defender portal by walking through the content displayed on the landing page. You'll also explore the options on the navigation panel that provide quick access to functionality that is part of Microsoft's Extended Detection and Response (XDR) solution: Microsoft Defender for Endpoints, and Microsoft Defender for Office 365 (email and collaboration). Lastly you'll also explore how Microsoft Secure Score can help an organization improve its security posture.

Task 1

Explore the Microsoft Defender landing page.

Open Microsoft Edge. In the address bar, enter admin.microsoft.com.

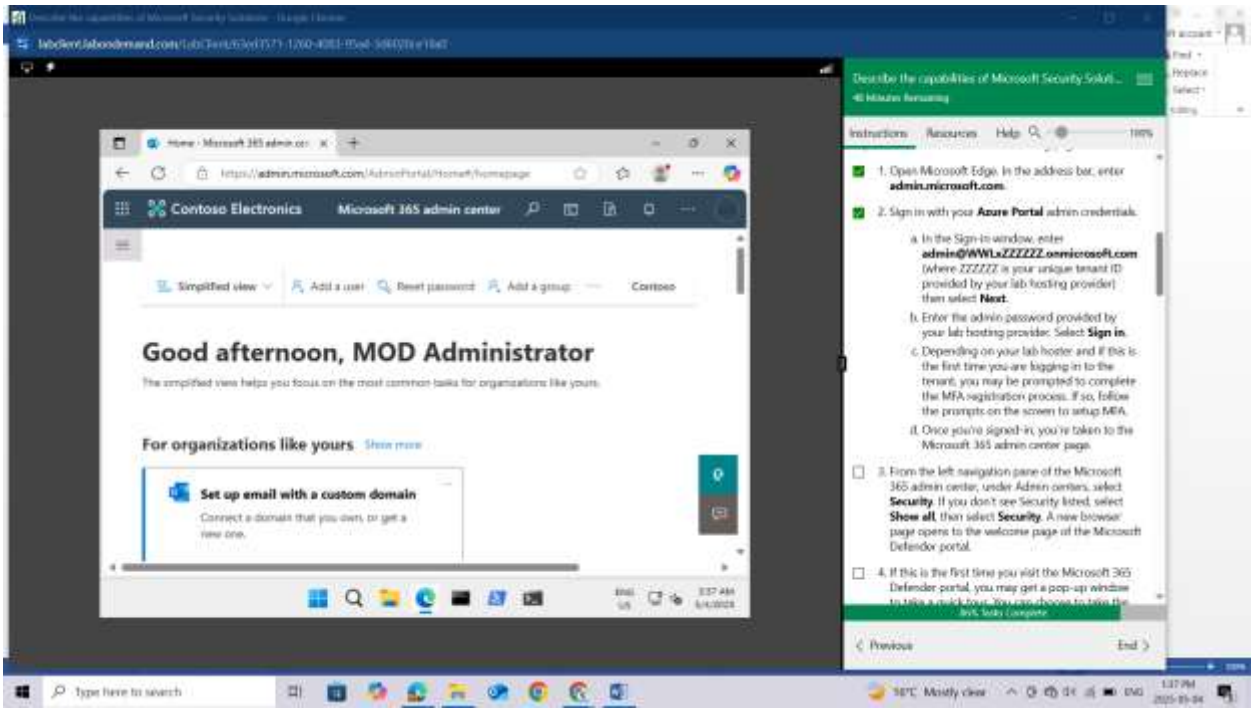
Sign in with your Azure Portal admin credentials.

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

Enter the admin password provided by your lab hosting provider. Select **Sign in**.

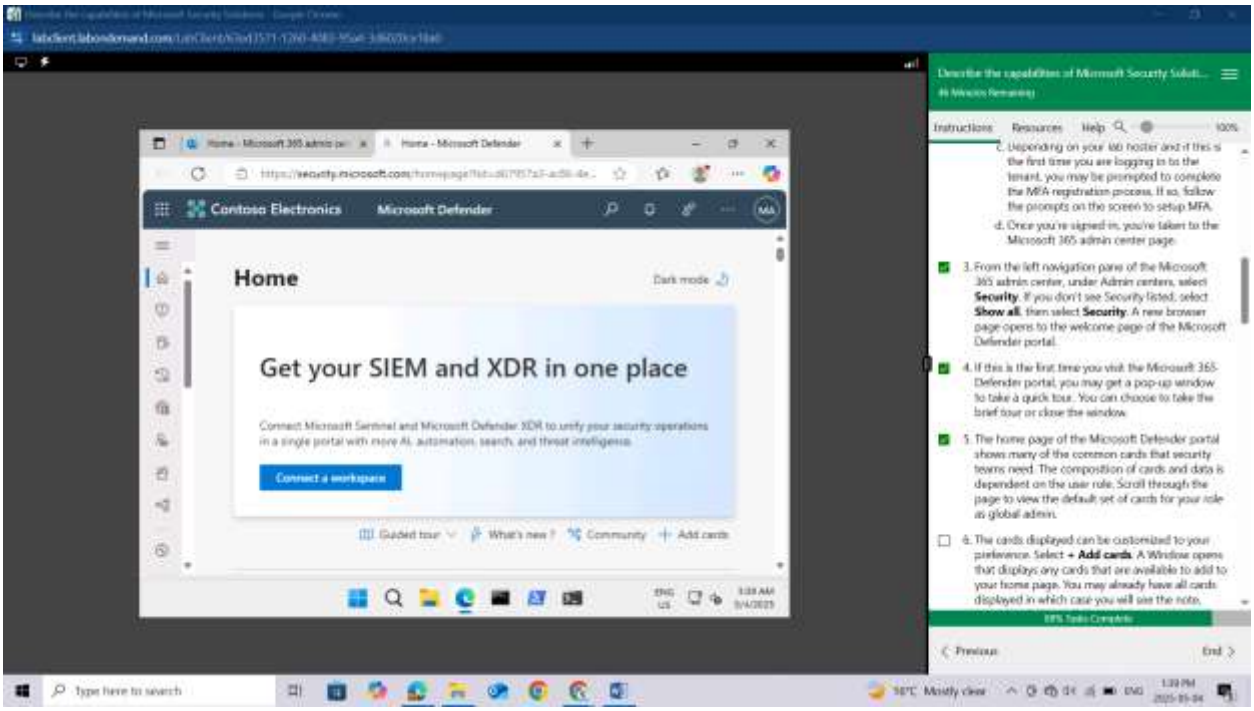
Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

Once you're signed-in, you're taken to the Microsoft 365 admin center page.

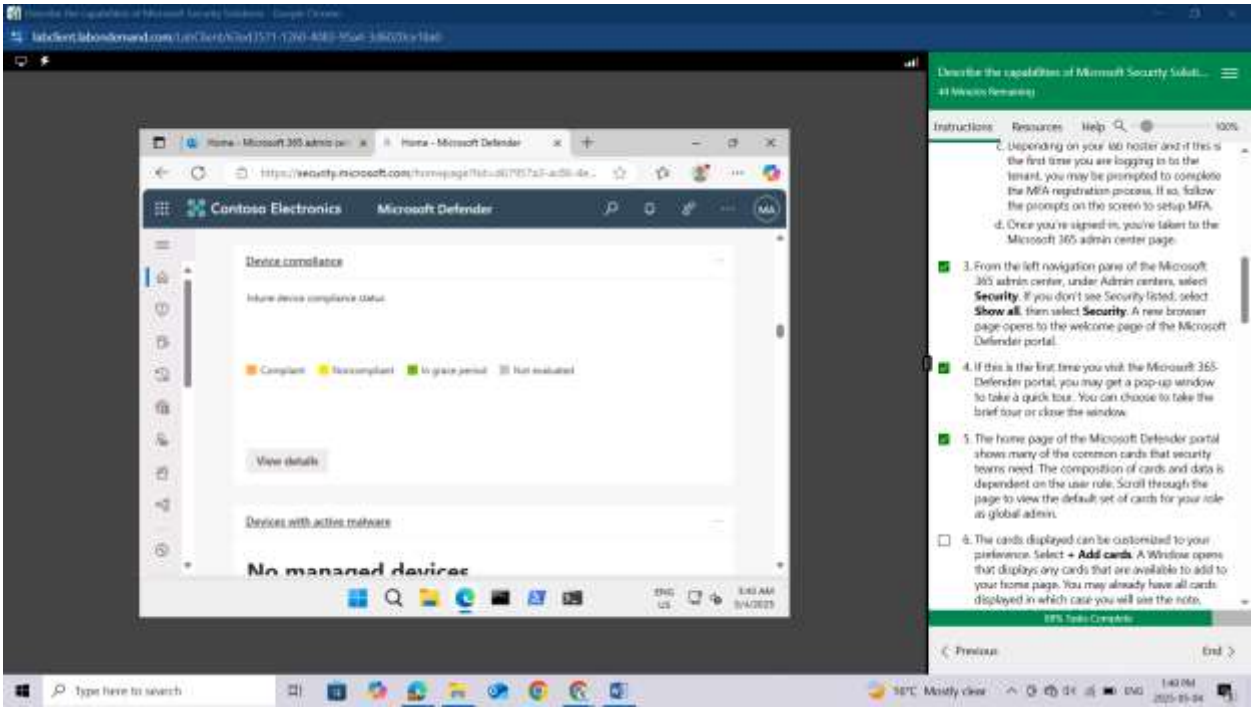


From the left navigation pane of the Microsoft 365 admin center, under **Admin centers**, select **Security**. If you don't see Security listed, select **Show all,** then select **Security**. A new browser page opens to the welcome page of the Microsoft Defender portal.

If this is the first time you visit the Microsoft 365 Defender portal, you may get a pop-up window to take a quick tour. You can choose to take the brief tour or close the window.

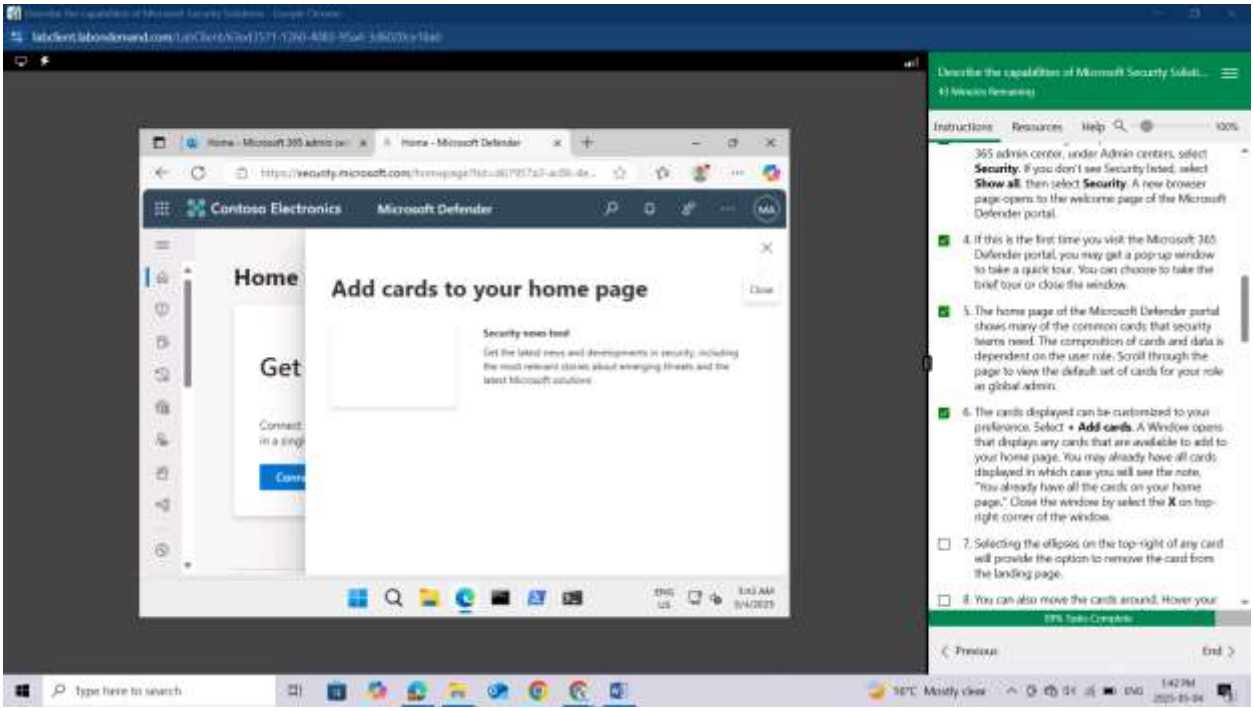


The home page of the Microsoft Defender portal shows many of the common cards that security teams need. The composition of cards and data is dependent on the user role. Scroll through the page to view the default set of cards for your role as global admin.

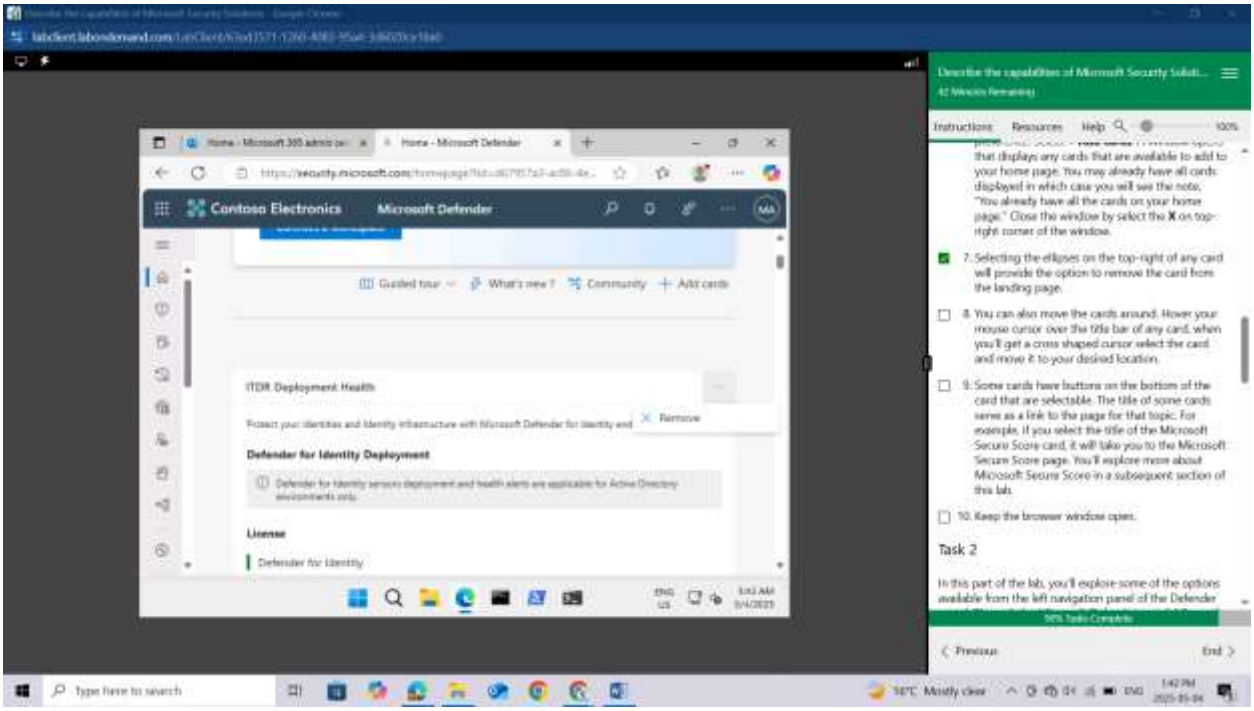


The cards displayed can be customized to your preference. Select **+ Add cards**. A Window opens that displays any cards that are available to add to your home page. You may already have all cards displayed

in which case you will see the note, "**You already have all the cards on your home page."** Close the window by select the **X** on top-right corner of the window.

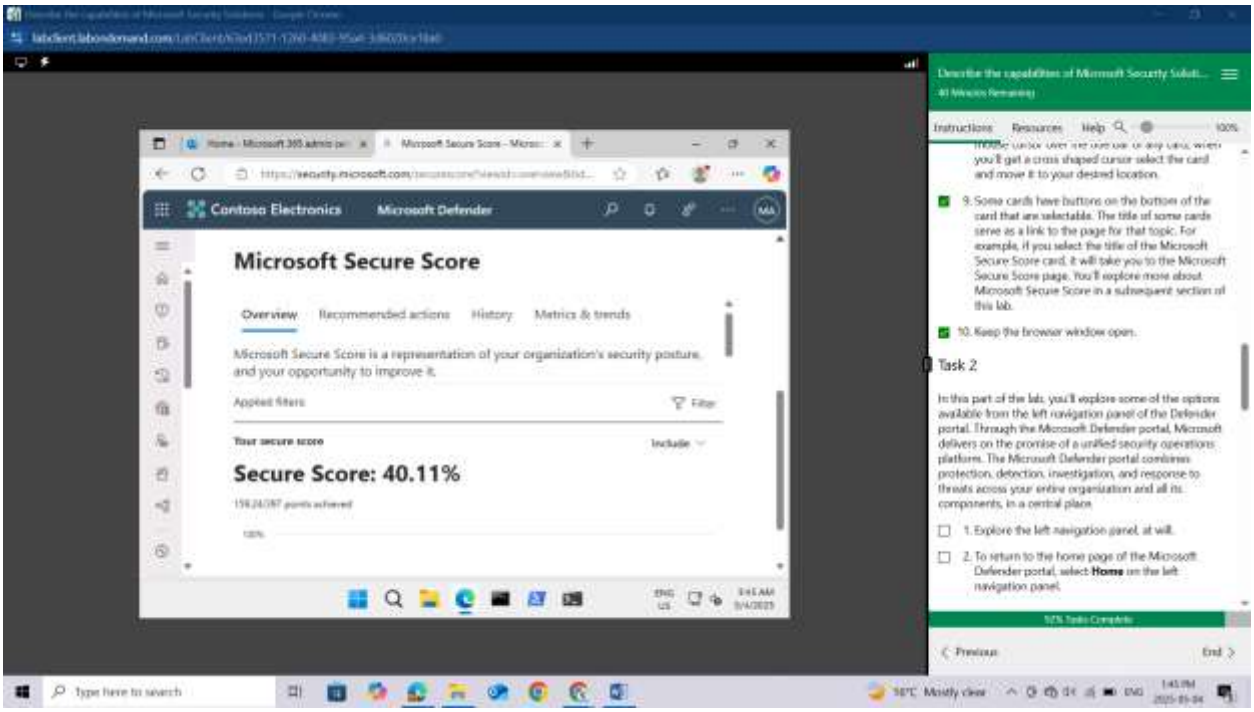


Selecting the ellipses on the top-right of any card will provide the option to remove the card from the landing page.



You can also move the cards around. Hover your mouse cursor over the title bar of any card, when you'll get a cross shaped cursor select the card and move it to your desired location. **I HAVE EXPERIENCED THE RELOCATION OF THE CARDS**

Some cards have buttons on the bottom of the card that are selectable. The title of some cards serve as a link to the page for that topic. For example, if you select the title of the Microsoft Secure Score card, it will take you to the Microsoft Secure Score page. You'll explore more about Microsoft Secure Score in a subsequent section of this lab.



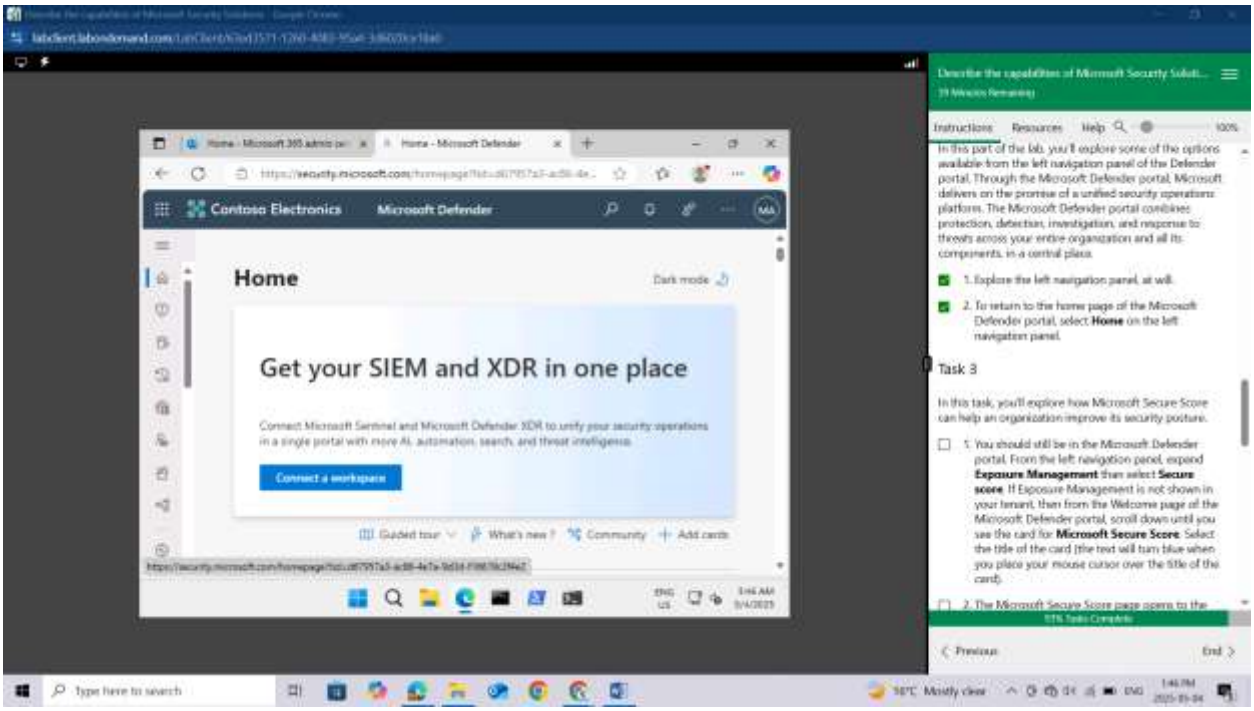
Keep the browser window open.

Task 2

In this part of the lab, you'll explore some of the options available from the left navigation panel of the Defender portal. Through the Microsoft Defender portal, Microsoft delivers on the promise of a unified security operations platform. The Microsoft Defender portal combines protection, detection, investigation, and response to threats across your entire organization and all its components, in a central place.

Explore the left navigation panel, at will.

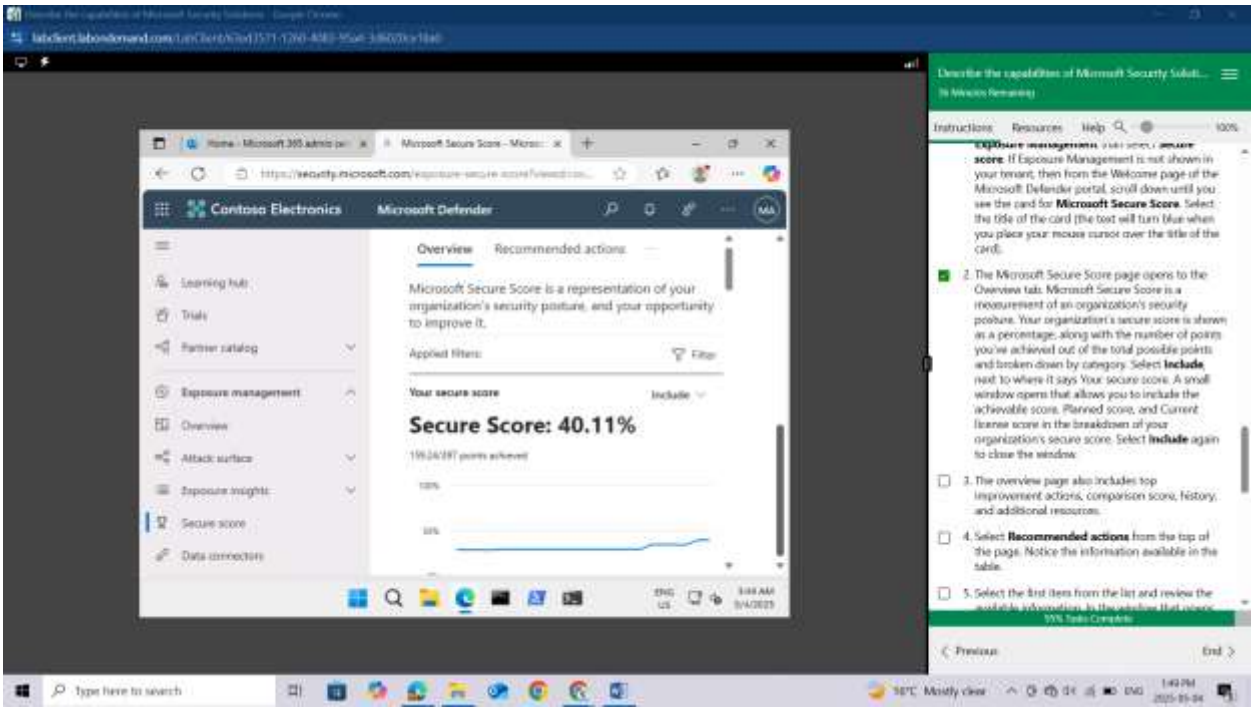
To return to the home page of the Microsoft Defender portal, select **Home** on the left navigation panel.



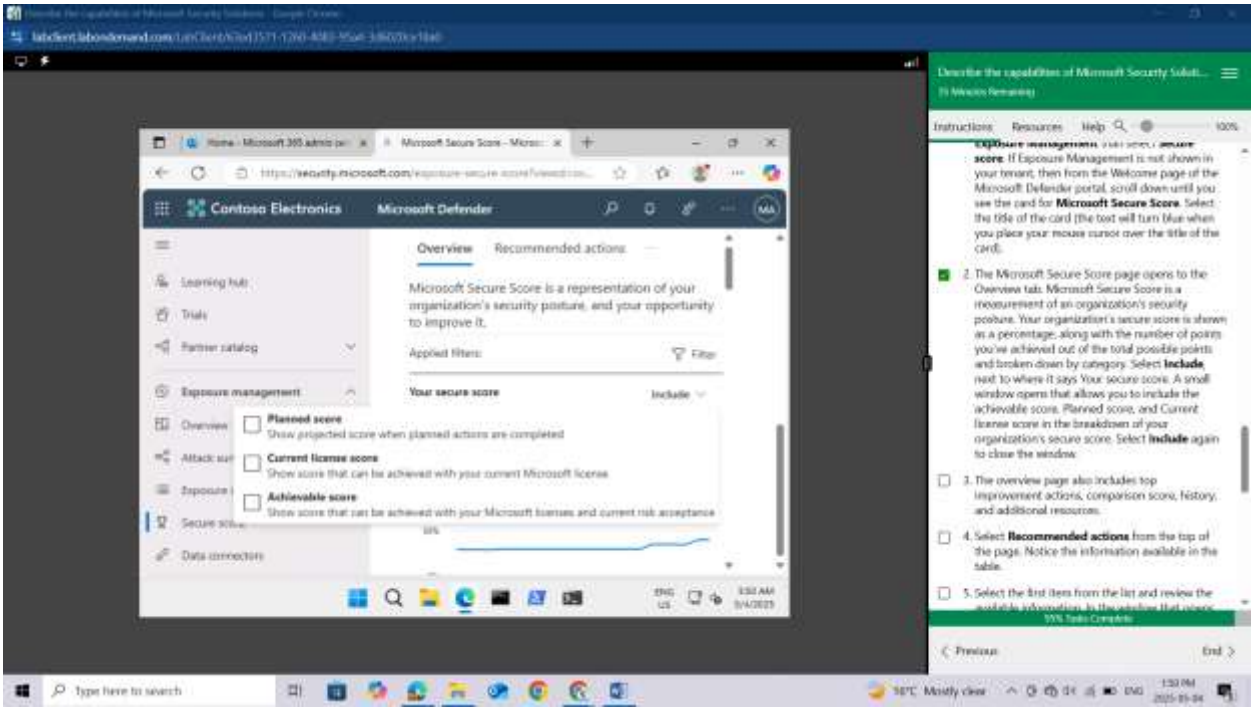
Task 3

In this task, you'll explore how Microsoft Secure Score can help an organization improve its security posture.

You should still be in the Microsoft Defender portal. From the left navigation panel, expand **Exposure Management** then select **Secure score.** If Exposure Management is not shown in your tenant, then from the Welcome page of the Microsoft Defender portal, scroll down until you see the card for Microsoft Secure Score. Select the title of the card (the text will turn blue when you place your mouse cursor over the title of the card).

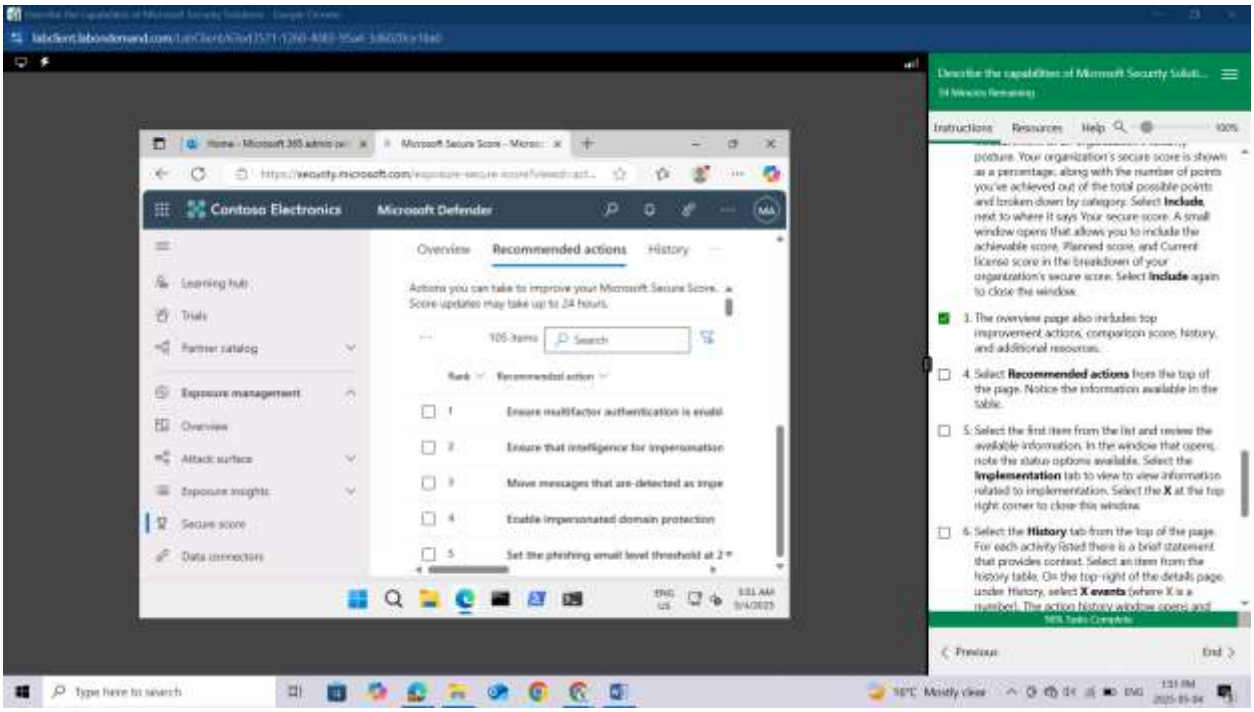


The Microsoft Secure Score page opens to the Overview tab. Microsoft Secure Score is a measurement of an organization's security posture. Your organization’s secure score is shown as a percentage, along with the number of points you've achieved out of the total possible points and broken down by category. Select **Include**, next to where it says Your secure score. A small window opens that allows you to include the achievable score, Planned score, and Current license score in the breakdown of your organization's secure score. Select **Include** again to close the window.

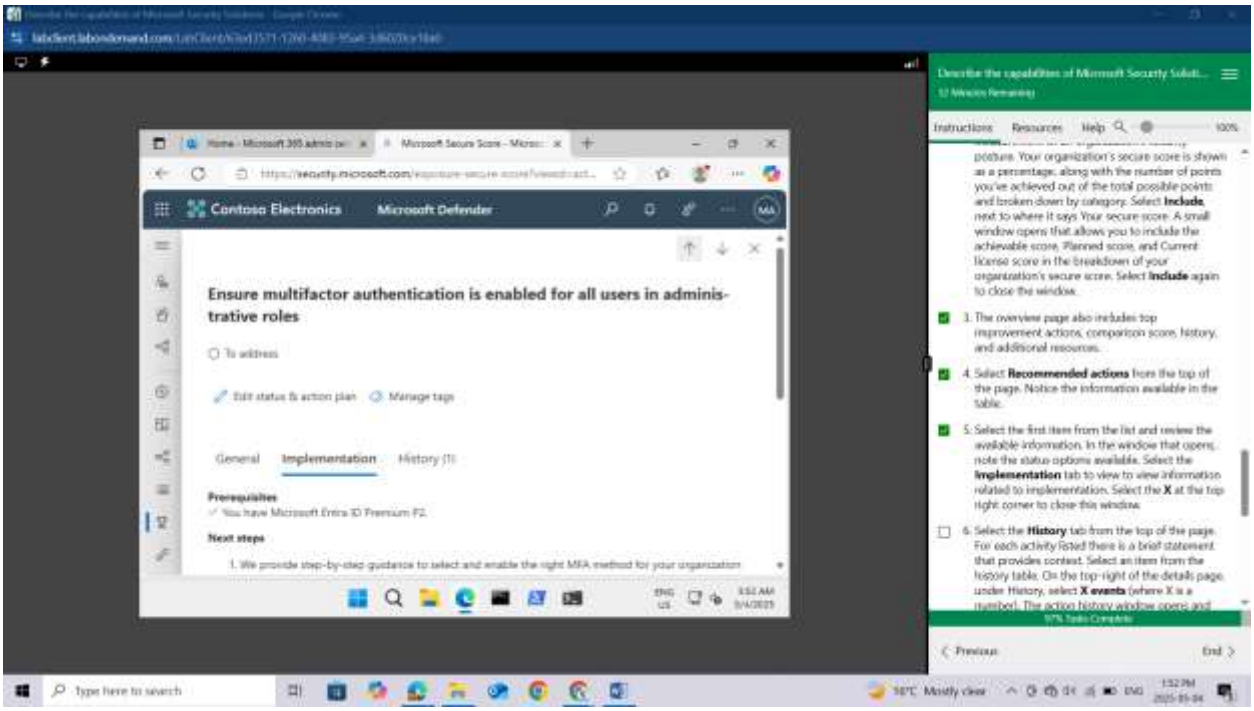


The overview page also includes top improvement actions, comparison score, history, and additional resources.

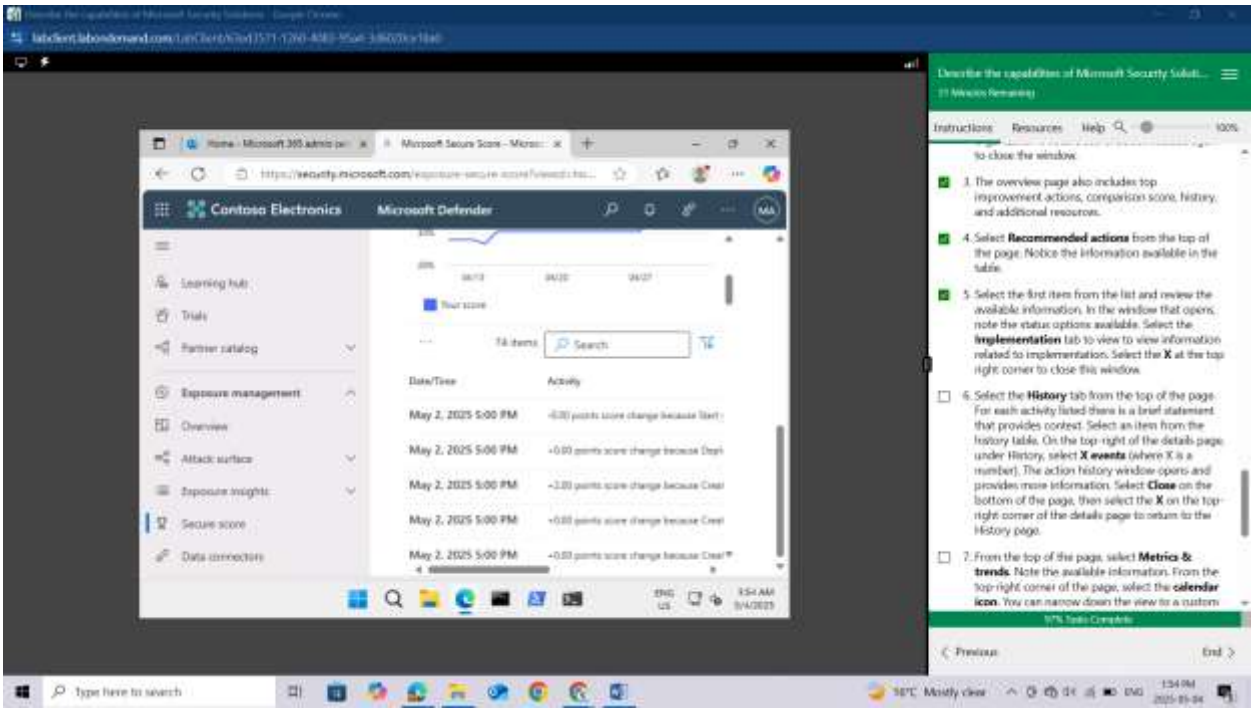
Select **Recommended actions** from the top of the page. Notice the information available in the table.



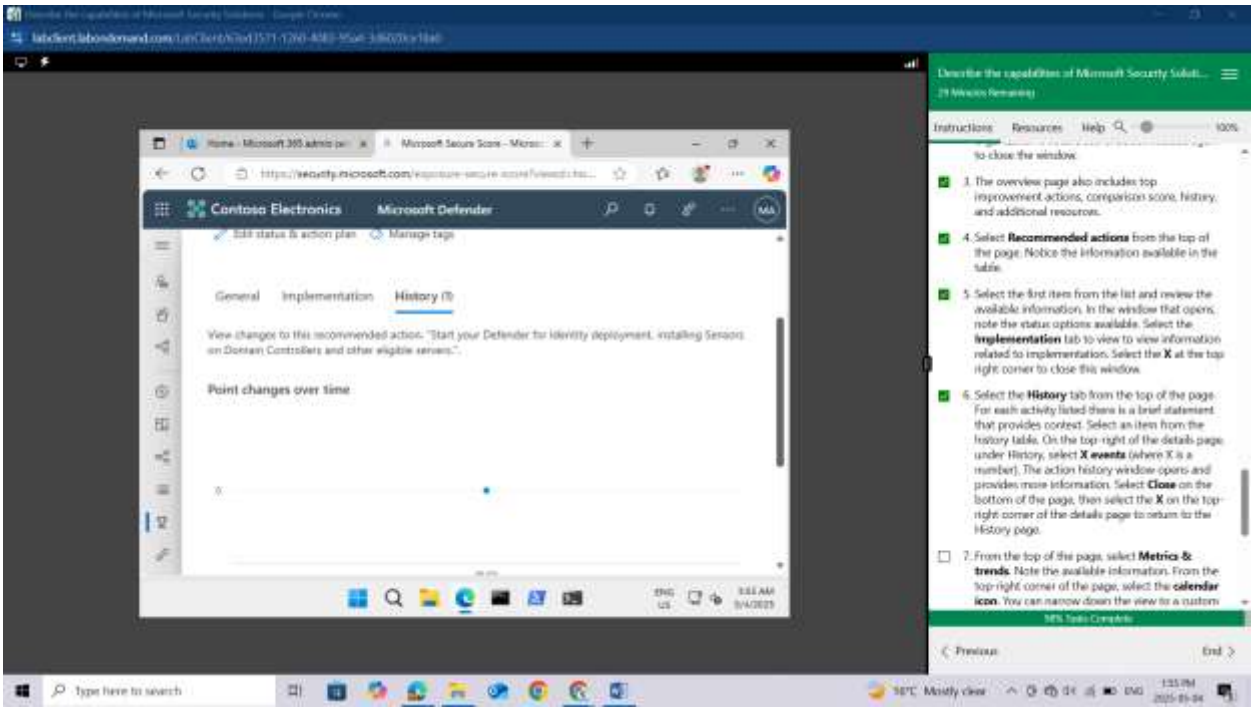
Select the first item from the list and review the available information. In the window that opens, note the status options available. Select the **Implementation** tab to view to view information related to implementation. Select the **X** at the top right corner to close this window.



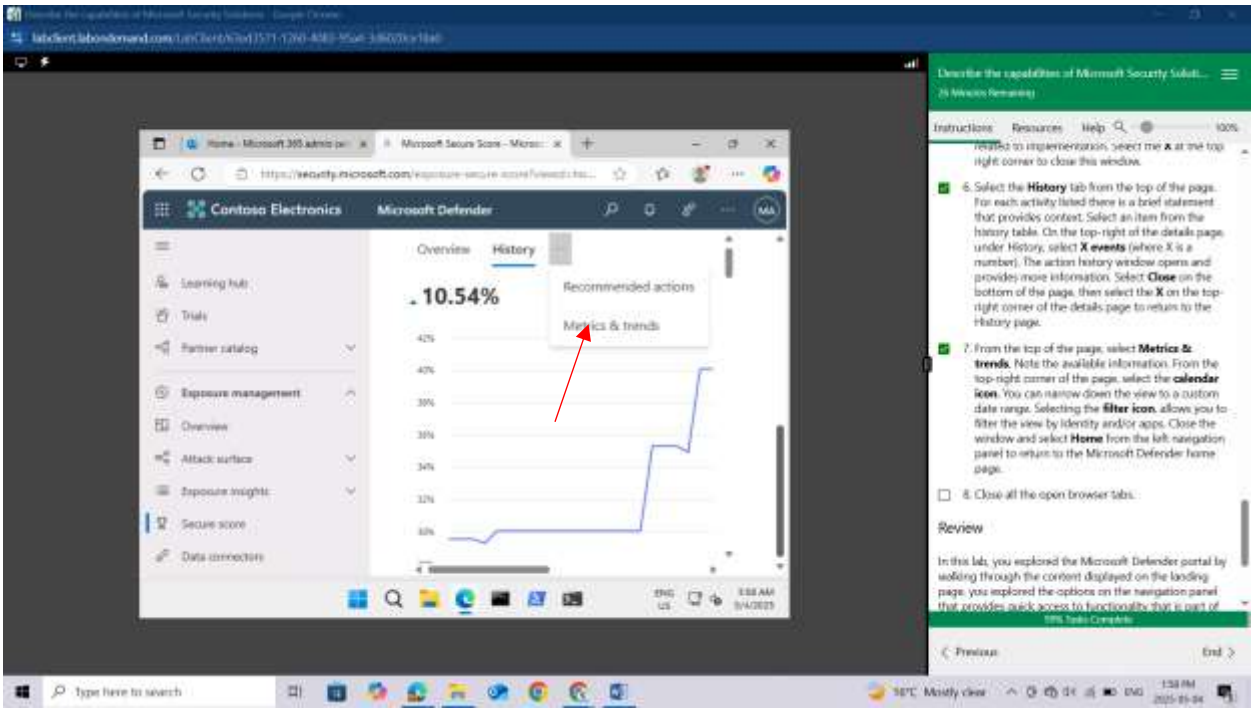
Select the **History** tab from the top of the page. For each activity listed there is a brief statement that provides context.



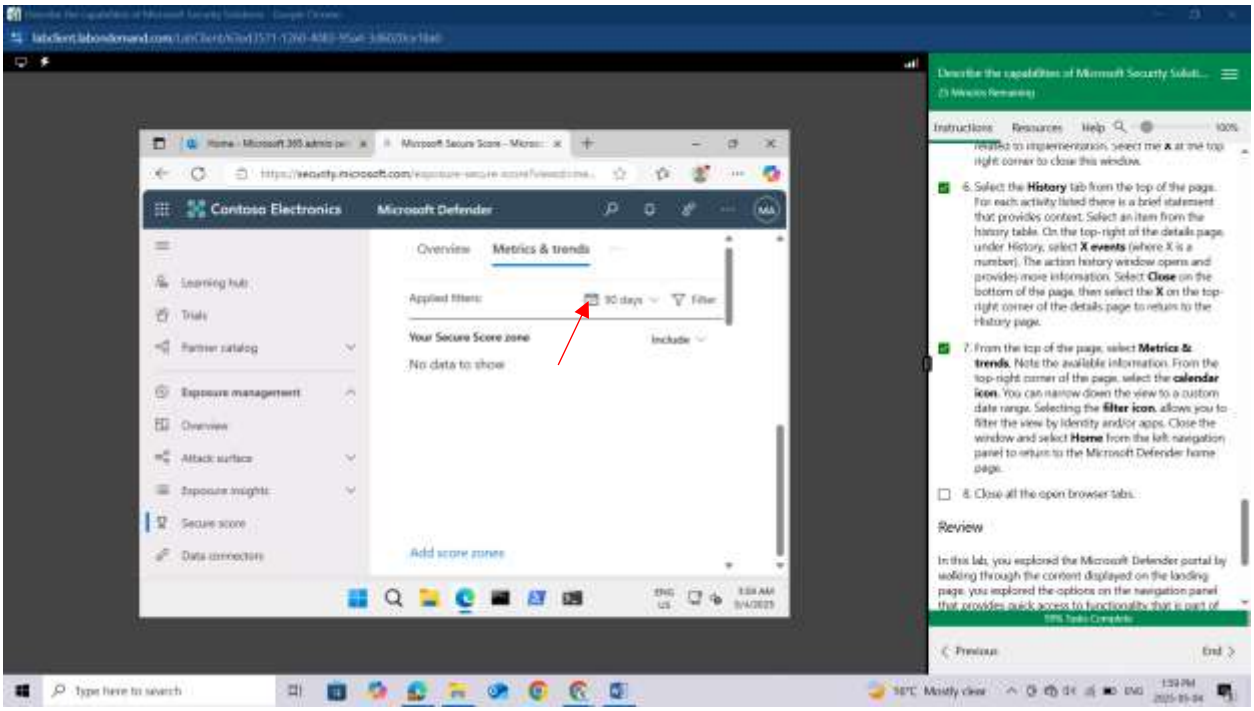
Select an item from the history table. On the top-right of the details page, under History, select X events (where X is a number). The action history window opens and provides more information. Select Close on the bottom of the page, then select the X on the top-right corner of the details page to return to the History page.



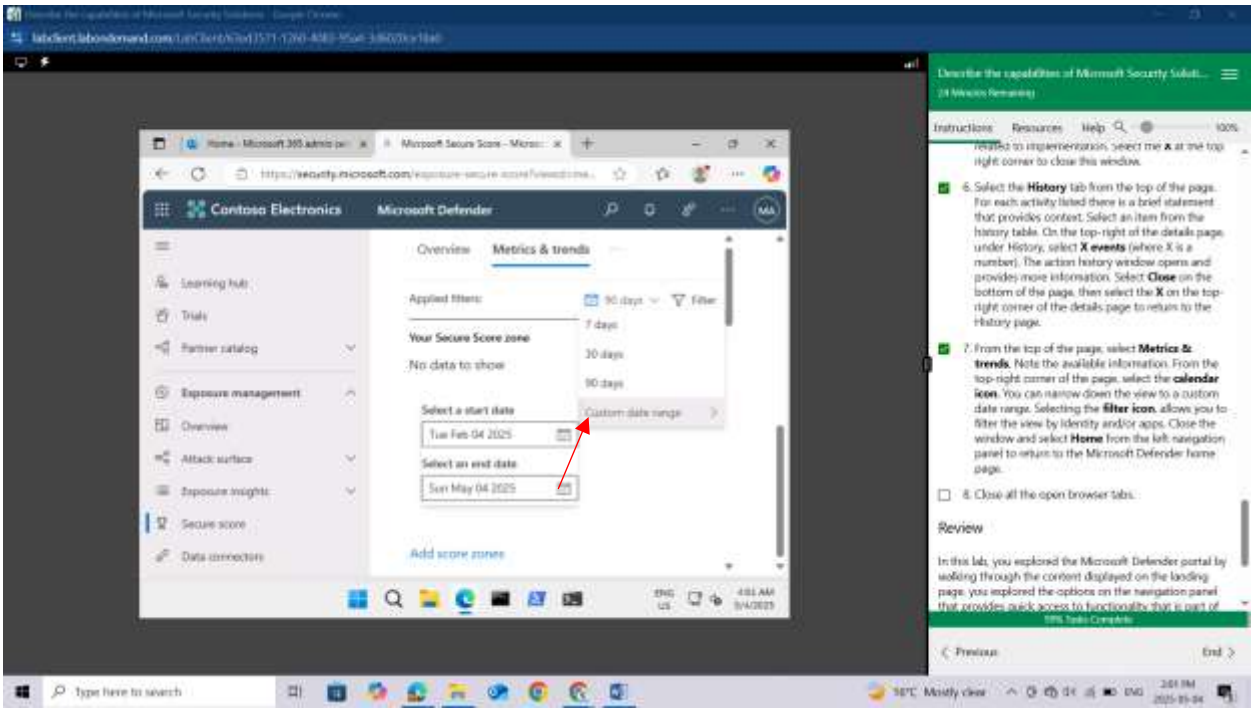
From the top of the page, select **Metrics & trends**. Note the available information.



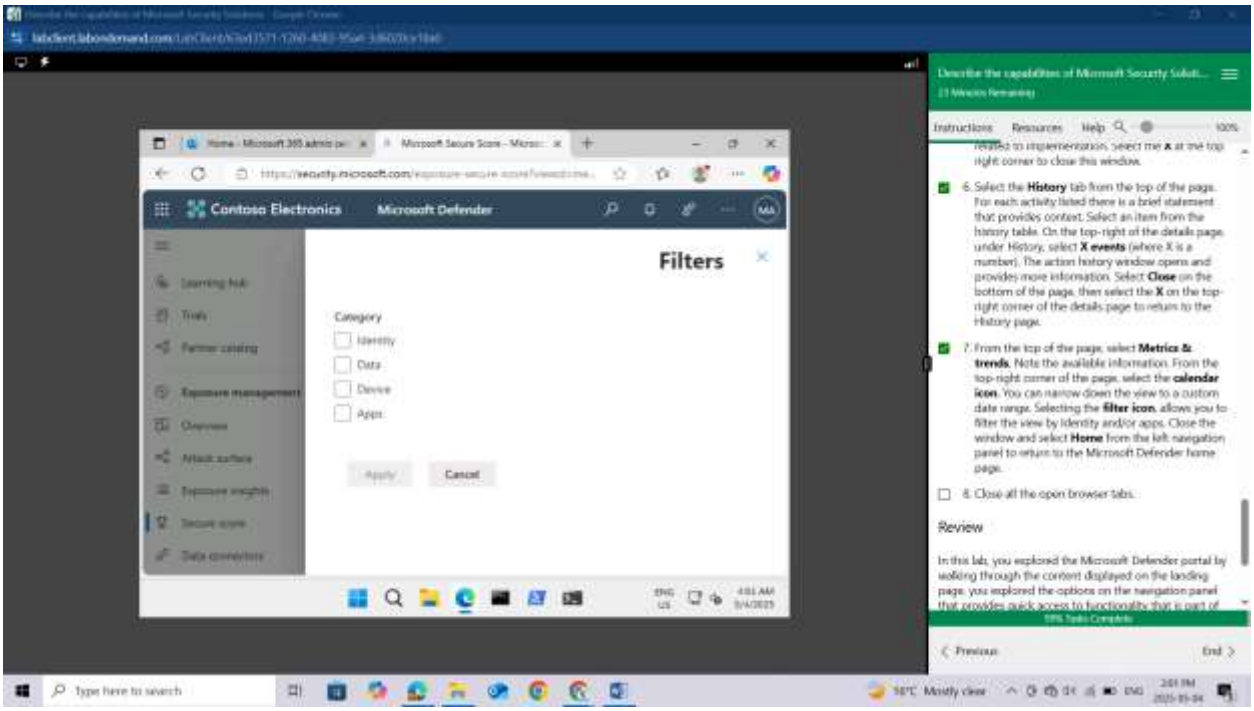
From the top-right corner of the page, select the **calendar** icon.



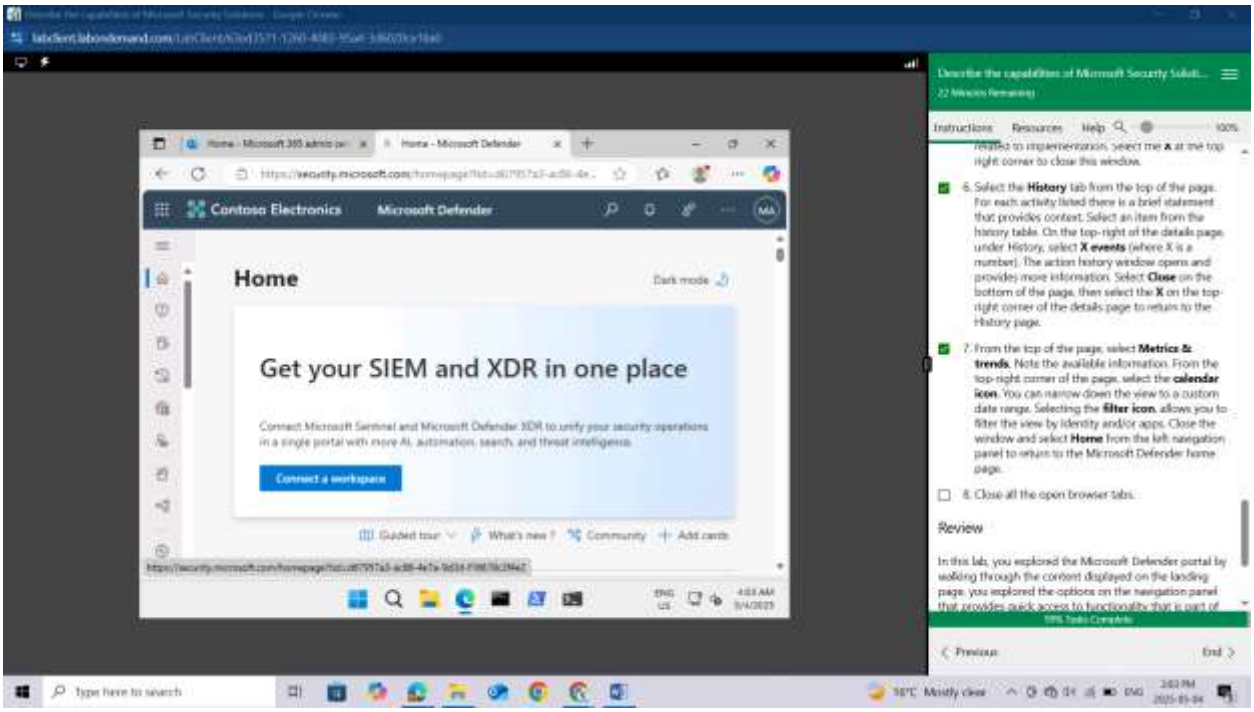
You can narrow down the view to a custom date range.



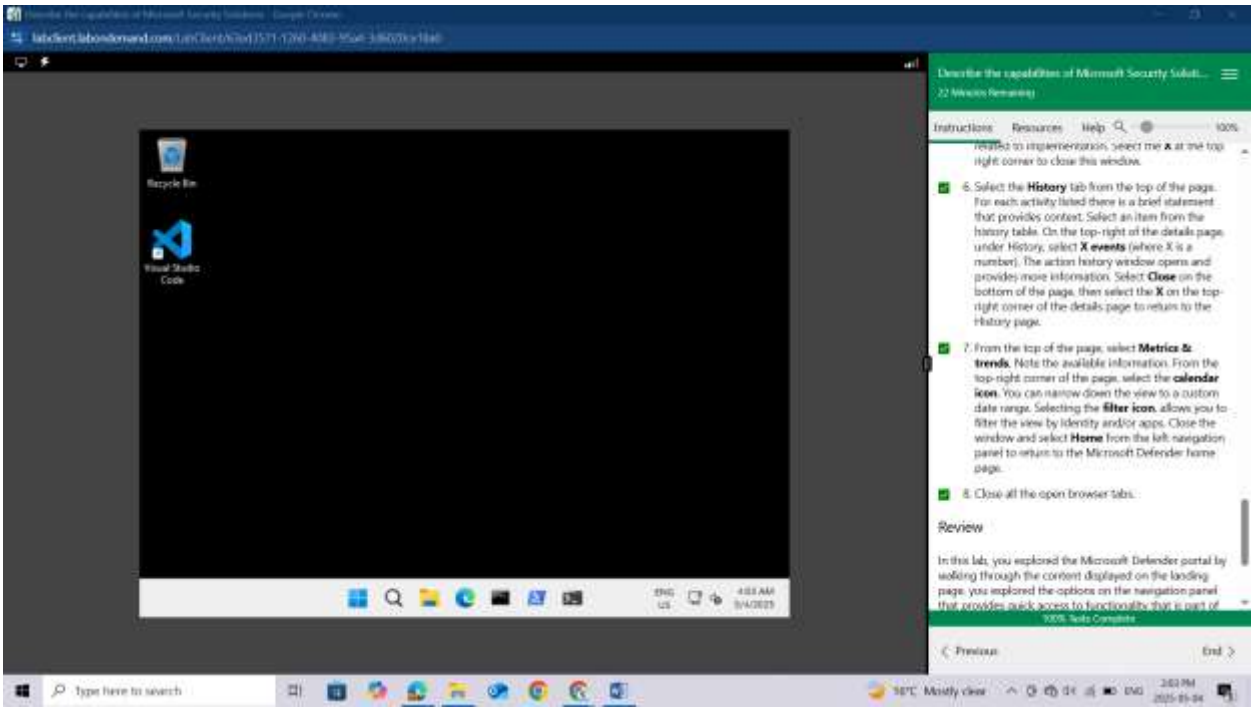
Selecting the **filter** icon, allows you to filter the view by Identity and/or apps.



Close the window and select **Home** from the left navigation panel to return to the Microsoft Defender home page.



Close all the open browser tabs.



Review

In this lab, you explored the Microsoft Defender portal by walking through the content displayed on the landing page, you explored the options on the navigation panel that provides quick access to functionality that is part of Microsoft's Extended Detection and Response (XDR) solution, Microsoft Defender for Endpoints, and Microsoft Defender for Office 365 (email and collaboration). Lastly you explored how Microsoft Secure Score can help an organization improve its security posture.

Conclusion

Through the Explore Microsoft Defender for Cloud Apps lab, I gained practical experience in achieving visibility and control over data and user activities within connected cloud applications, emphasizing data protection and governance. Also went through the Explore the Microsoft Defender portal lab, which showcased its role as a centralized hub for managing security across the Microsoft 365 environment, providing a unified view of alerts, threats, and overall security posture. Together, these labs highlighted Microsoft's integrated approach to securing cloud application usage and centrally managing the broader security landscape.