

## Copilot for Security – Hands on Workshop Lab Guide (United Kingdom Workshop)



## Copilot for Security – Hands on Workshop Lab Guide (United Kingdom Workshop)

### Table of Contents

Activity 1: Let's Get Familiar with Copilot for Security .....	2
Exercise 1: Copilot for Security Standalone Experience.....	2
Explore Copilot for Security Standalone Experience. ....	2
Activity 2: Prompting Use Cases .....	8

Exercise 1: Effective Prompting.....	8
Effective vs non effective prompts .....	8
Building and iterating on your prompt.....	10
Exercise 2: Investigate an identity-based security incident.....	10
Investigate in standalone .....	10
Activity 3: Embedded .....	11
Exercise 1: M365 Defender .....	12
Incident Summary and Guided Response.....	12
Incident Report .....	13
File Analyzer .....	14
Script Analyzer .....	15
Device Summary .....	15
Activity 4: Intune Use Cases .....	17
Exercise 1: Intune Policy Management with conflict analysis.....	17
Exercise 2: Summarize Existing Policies & Assess their Impact to users & Security.....	21
Exercise 3: Assistance to troubleshoot devices .....	23
Exercise 4: Compare devices for troubleshooting.....	26
Exercise 5: Analyzing error codes .....	28
Exercise 6: Advanced analyzing using KQL query .....	30
Activity 5: Purview Use Cases .....	32
Exercise 1: Data Loss Prevention.....	32
Exercise 2: Insider Risk Management.....	37
Activity 6: Entra Use Cases .....	44
Exercise 1: Sign-logs Investigation.....	44
Exercise 2: Risky users summarization .....	46

# Activity 1: Let's Get Familiar with Copilot for Security

## Exercise 1: Copilot for Security Standalone Experience

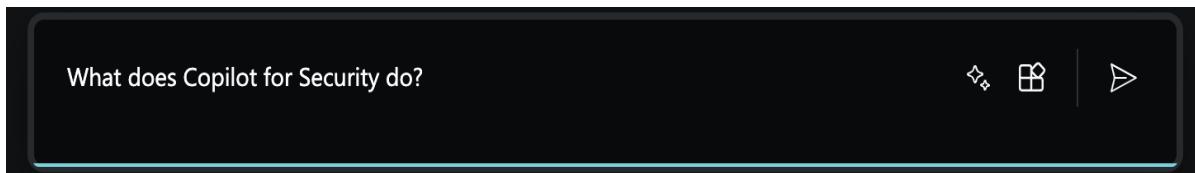
In this exercise, you will explore the Copilot for Security Standalone Experience. You will learn how to navigate the portal, manage plugins, and utilize various features to enhance your security operations. This hands-on activity will help you become familiar with the capabilities of Copilot for Security and how to effectively use it in your security workflows.

### Explore Copilot for Security Standalone Experience

1. Open your browser, and go to the Copilot for Security at <https://securitycopilot.microsoft.com/>
2. Select the  **home menu** in the left corner
  - a **My sessions** view on past sessions you created
  - b **Account** Ensure that you are signed in with your Alpine Ski house account. If it shows a different account, you need to sign out and sign in with the correct account.
  - c **Settings** include theme, time zone, and language preferences along with some settings for Copilot owners.

 **Important Remark:** *Since your account has the Contributor role in Alpine Ski House, not all options are visible. Owners can manage capacity, data evaluation, see usage and more.*

3. You will find the **prompt bar** at the bottom of the Copilot home page. To ensure everything is working correctly, you can use a test prompt: **What does Copilot for Security do?**



4. Select **Send**  or press Enter. Wait for Copilot for Security to generate a response.
5. **Expand Steps Completed.**

 **Tip:** Notice the plugin selected was 'Microsoft Documentation' by the Copilot for Security

*Orchestrator.* Microsoft Copilot orchestrator works behind the scenes to select and execute the right plugin and skill(s).

q

What does Copilot for Security do?

3 steps completed 40 seconds

> Chose Microsoft Documentation 8 seconds

> Searched documentation 19 seconds

> Prepared your response 13 seconds

6. At any time during a Copilot for Security session, you can share your session with users in the same tenants. Select to create a link.
  7. The icon in the prompt bar is used to manage **plugins**. You can toggle plugins on or off and configure them. We will get into more details later.
- Tip:** Plugins extend Copilot's capabilities by integrating with various security products from Microsoft or third-party providers. Think of Microsoft Copilot for Security like a smartphone, and the plugins are the apps you install to enhance its functionality.
8. Look for the sparkle icon next to the prompt bar icon to use the search to find capabilities, also referred to as **skills**. Select **See all system capabilities** to see all the prompts listed for each plugin.

≡ SYSTEM CAPABILITIES  See all system capabilities >

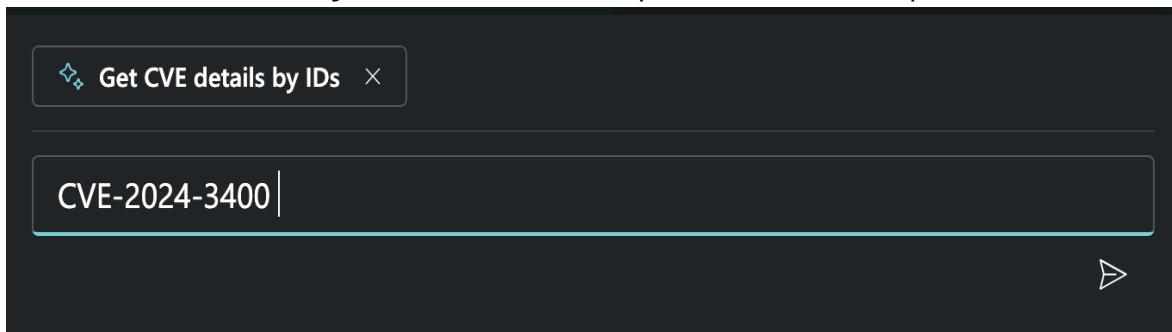
Capabilities are based on the plugins you have set up.

**Analyze a script or command**  
Analyze and interpret a command or script to natural language.

**Analyze security data**  
Analyze, summarize, and explain security data such as event logs, and answer security questions.

**Convert Unix Timestamp**  
Convert a Unix timestamp to a human readable date and time.

9. In the search bar, type **CVE** and reveal all the skill (set of function) that reside inside the Microsoft defender threat intelligence plugin.
10. Let's select “**Get CVE by ID**” and review the input that this skill required.



11. In the input parameter add the, **CVE-2024-3400** and press run.
-  **Tip:** By selecting the capability Copilot invoked the skill directly without using the Orchestrator.
12. Using the same sparkle icon, you can see a list of **promptbooks** that you can start with.
-  **Tip:** Promptbooks are collections of prompts designed to accomplish specific security tasks. They run a series of prompts in sequence, with each prompt building on the previous one.

Search

---

**Get started using these examples**

 **PROMPTBOOKS**  See all promptbooks >

Promptbooks are sets of prompts that run in sequence automatically.

**Analyze Microsoft Sentinel Incident**

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

13. You can also select **View promptbook library** on the home page or via the settings menu. We will explore promptbooks in more depth later.

Copilot for Security comes with many preinstalled plugins available for Microsoft security services and other commonly used services and websites that you can use. You also have the option of extending default capabilities by adding your own custom plugins and non-Microsoft plugins as shown below:

1. The icon  in the prompt bar is used to **manage plugins**. You can toggle plugins on or off and configure them.
2. Select the plugin you'd like to use by turning the toggle on or off. For this lab make sure the **following plugins are toggled on**:
  - Microsoft Entra
  - Microsoft Defender XDR
  - Microsoft Defender Threat Intelligence
  - Microsoft Intune
  - Microsoft Purview
  - Microsoft Sentinel

 **Tip:** Copilot for Security some plugins need to be personalized by configuring the plugin setting. For example, for the Microsoft Sentinel plugin the default workspace needs to be provided..This has been already setup for the Alpine Ski house tenant.

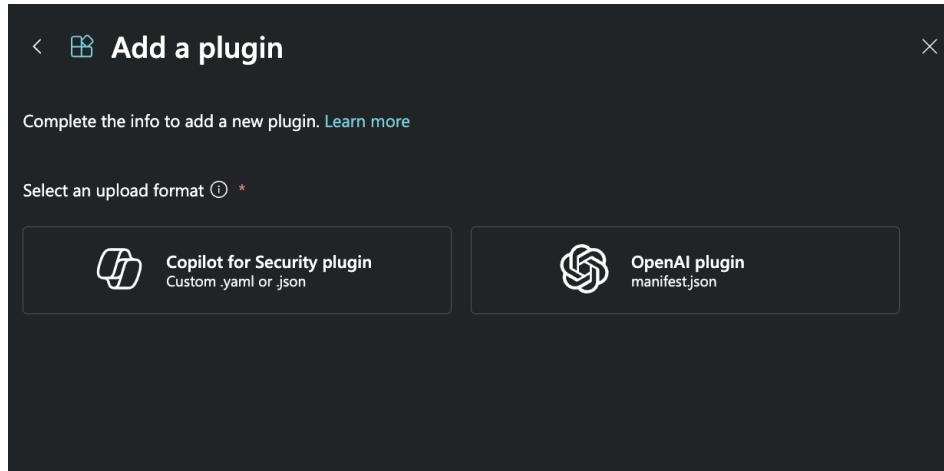
The screenshot shows the 'Manage sources' interface with the 'Plugins' tab selected. A search bar and filter buttons for 'All (29)', 'On (10)', and 'Off (19)' are at the top. Below is a list of Microsoft security services as plugins:

Service	Description	Status
Microsoft Defender External Attack Surface Management	Attack surfaces, vulnerable assets, and attack surface insights	On
Microsoft Defender Threat Intelligence	Articles, intelligence profiles, vulnerabilities, indicators of compromise, hosts, and threat analytics	On
Microsoft Defender XDR	Alerts and incidents	On
Microsoft Entra	Alerts, users, groups, access reviews, and risky services	On
Microsoft Intune	Devices, apps, policies, and postures	On
Microsoft Purview	Purview alerts, Insights, and Risk details	On
Microsoft Sentinel (Preview)	Incidents and workspaces	On

3. In Manage plugins, scroll down to the **Custom section**.
4. Select, **Add plugin**.

**⚠️ Important Remark:** This option is available because the Owner has configured Copilot for Security to allow Contributors to add and manage custom plugins for everyone in the organization. the custom plugin will available to just yourself. Owners can decide to upload a plugin for themselves or anyone in the organization.

5. From the drop-down options, choose between adding a **Copilot for Security plugin** or **an OpenAI plugin**.
6. Depending on the plugin you'd like to add choose **to upload a file or upload as a link**.



7. After the plugin is successfully added, some plugins might need to be set up. You can also choose to set up the plugin later.
8. You will find the **prompt bar** at the bottom of the Copilot home page. To ensure everything is working correctly, you can use a test prompt: **Who am I?**
9. Select **Send**  or press Enter. Wait for Copilot for Security to generate a response.
10. **Expand Steps Completed.**

## Activity 2: Prompting Use Cases

Estimated time to complete this activity

30 minutes

### Exercise 1: Effective Prompting

In this lab, we will practice creating effective prompts for Microsoft Copilot for Security. A prompt is the text you type to instruct Copilot on what you need. The quality of the response from Copilot largely depends on how clear and specific your prompt is.

*The Prompts! Good input = good output. Imagine you are instructing a junior security assistant. The more specific you are, the better they can help you.*

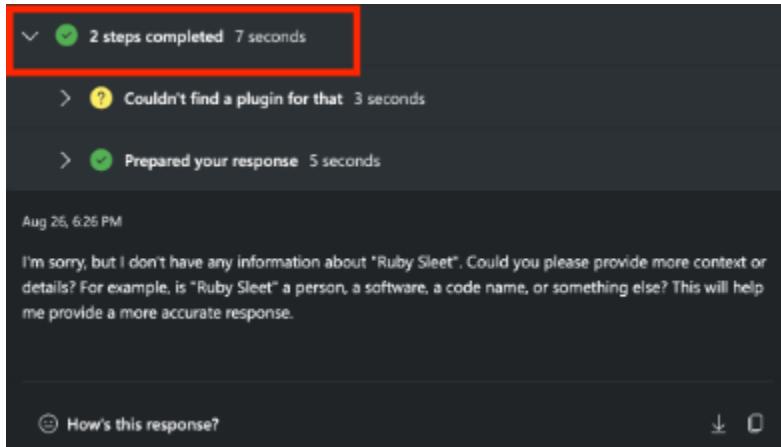


### Effective vs non effective prompts

In this exercise, you will learn the difference between ineffective and effective prompting by comparing two different approaches to querying information. You will also learn about common issues and mistakes when prompting Copilot for Security. Understanding these mistakes will help you and your customers craft more effective prompts and get better responses from Copilot.

#### Ineffective Prompt

1. If you have written an inaccurate prompt you may receive an inaccurate response or a message similar to below:



## Effective Prompt

1. Starting a new session type, **Can you give me information about Pearl Sleet activity, including a list of known indicators of compromise and tools, tactics, and procedures (TTPs)?** Wait for Copilot for Security to generate a response.
2. Expand steps completed and **review the selected plugin.** Notice that Copilot has now selected the Microsoft Threat Intelligence plugin and provided an answer.
3. Starting a new session type, **Write a report about a Microsoft XDR incident number 2807 that can be reviewed by my SOC manager.** Wait for Copilot for Security to generate a response.
4. Expand steps completed and **review the selected plugin.** Notice that Copilot has now selected the Microsoft Defender XDR plugin and provided an answer.
5. Starting a new session type, **Give me a list of high-risk unmanaged devices in my network from Microsoft Intune. If they're named "test", remove them from the list.** Wait for Copilot for Security to generate a response.
6. Expand steps completed and **review the selected plugin.** Notice that Copilot has now selected the Microsoft Intune plugin and provided an answer.

**Tip:** If Copilot is unable to provide an answer, consider that the required plugin might be disabled. Check the plugin management settings to ensure that the necessary plugin is toggled on.

## Building and iterating on your prompt

This exercise focuses on building and iterating on your prompts to create effective queries for Copilot for Security.

 **Tip:** It's important to note that crafting the perfect prompt often takes a few iterations, and that's perfectly okay. You don't need to have a long, detailed prompt in one go. Instead, you can break it down into multiple separate prompts and refine it as you go. The below example is to show you how to tailor your prompts and get a more specific response.

1. Start a new session and in the prompt bar type **Give me a summary of Defender incident 889**. Specifying the source can help get more accurate responses. Additionally, In real life a customer might have multiple incident systems.
2. Now further iterating, we can add the needed incident details. **Give me a summary of Defender incident 889 and list the entities involved**.
3. Being specific about the format and focus of your request can make the response better suited to your needs. **Give me a summary of Defender incident 889 and list the entities involved. Compile the information in a table and add a summary**.
4. By Tailoring the information to your audience, you can effectively communicate complex incident details in a way that is accessible and understandable to everyone. **Give me a summary of Defender incident 889 and list the entities involved. Compile the information in a table and start with a summary for a non technical audience**.

## Exercise 2: Investigate an identity-based security incident.

In this exercise, you will investigate a potential identity-based security incident. You have received an alert indicating suspicious activity from a user account [irvins@vnevado.alpineskihouse.co](mailto:irvins@vnevado.alpineskihouse.co) that has been flagged as a risky user.

### Investigate in standalone

 Disclaimer: All: Please note that environments are constantly changing. As a result, you may not always receive responses for the specific user you have selected. The information provided is based on the most recent data available, and user statuses may

change over time.

1. As a security analyst at Alpine Skihouse, you start a new session to investigate a specific user. You type: **Can you show me the list of users flagged as risky in the last 14 days?**
2. From the list, select a user with a high-risk level. For example, you might choose [jonaw@vnevado.alpineskihouse.co](mailto:jonaw@vnevado.alpineskihouse.co), type: **Tell me about user [jonaw@vnevado.alpineskihouse.co](mailto:jonaw@vnevado.alpineskihouse.co) from Entra.** Copilot provides you with basic information about the user, including their role. You decide to dig deeper into the user's risk profile.
3. You type: **What is the risk level, state, and risk details for the above user?** Copilot responds with a detailed overview of risky activities associated with the user.
4. Next, you want to know about the user's recent sign-in activities. You type: **When did the above user last sign in, and to what target application?** Copilot provides the last sign-in time and the application accessed, giving you insight into the user's recent behavior.
5. To understand the user's security setup, you type: **What authentication methods are set up for the above user?** Copilot lists the authentication methods, such as multi-factor authentication (MFA) or no password sign-in, that are configured for the user.
6. You then check for any failed sign-in attempts. You type: **Did the above user have any failed sign-ins during the last 14 days?** If yes, list the location and IP address of each failed sign-in attempt." Copilot provides a list of failed sign-ins, including the locations and IP addresses, helping you identify any unusual patterns.
7. To complete your investigation, you need to review the user's audit logs. You type: **Show audit logs for the above user for the last 14 days.** Copilot generates a summary of the audit logs, detailing the user's activities and any significant events.

Using Copilot for Security, you gathered comprehensive information about the user, including sign-in activities, audit logs, and risky user detections.

8. After completing your investigation, a Tier 2 analyst needs to take action to remediate or unblock the risky user. In the same session, you type: **Write a report based on this investigation. Provide your assessment of the user's risk level with supporting evidence and confidence level. List the most notable facts from this session as bullet points, along with supporting reasons. The audience is a Tier 2 SOC analyst who needs to take action to remediate or unblock the risky user. Include recommendations on how to proceed with user risk remediation in Entra.**

## Activity 3: Embedded

Estimated time to complete this activity

30 minutes

The objective of this activity is to familiarize participants with Copilot for Security embedded features and demonstrate the value they bring. Through hands-on exercises, participants will learn search for incidents, review summaries, analyze scripts and files, summarize device information, use guided responses to resolve incidents, generate KQL queries, and create incident reports. Additionally, participants will gain experience with Intune and Purview, managing policies, troubleshooting devices, and summarizing Insider Risk Management alerts.

## Exercise 1: M365 Defender

This exercise involves investigating a Human Operated Ransomware attack using Microsoft Defender and Copilot for Security. You'll search for the incident, review the summary, analyze scripts and codes, analyze files, summarize device information, use guided responses to resolve incidents, generate KQL queries and create incident reports.

### Incident Summary and Guided Response

1. Go to **Investigation & response > Incidents & alerts > Incidents on** in the [Microsoft Defender portal](#)
2. In the incident search bar, start typing "**Human-Operated Ransomware**" and hit enter

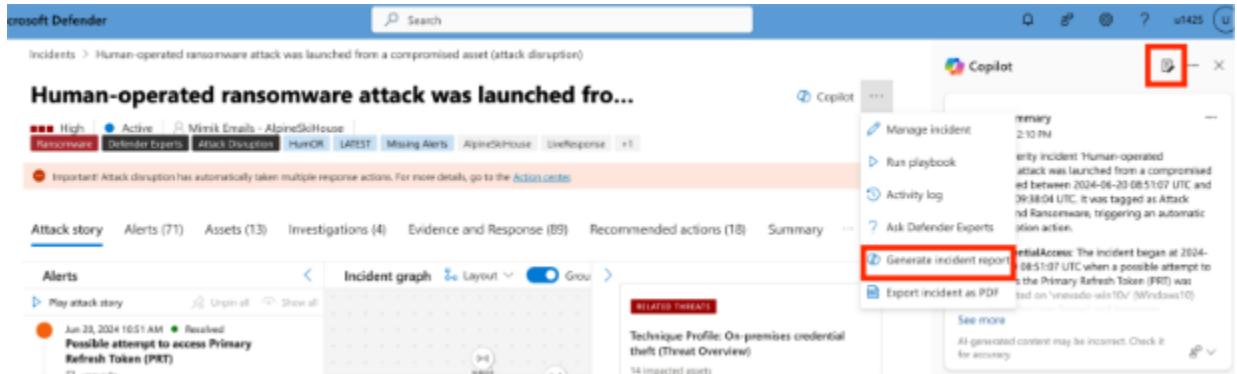
The screenshot shows the Microsoft Defender portal's incident search interface. A red arrow points to the search bar at the top right, which contains the text "human-operated ra...". Below the search bar are several filter options: Status: Any, Alert severity: Any, Incident severity: Any, Incident assignment: Any, Incident name, Incident Id, Tags, Severity, and Investigation. A specific search result is highlighted: "Human-operated ransomware attack was launche... 107". This result is categorized under "Ransomware" with a count of "+8", "High" severity, and "3 investigat...".

3. Open the incident page by clicking on it >Copilot automatically creates an **Incident Summary** upon opening the page.  
**Tip:** Review the generated summary and involved files.
4. The Copilot pane appears on the right side also shows the **Guided Response cards**.  
**Tip:** Each card contains information about the recommended action, including the entity where the action needs to be applied and why the action is recommended. The cards also emphasize when a recommended action was done.
5. **Close the generated summary** by clicking the "X" button located at the top-right corner of the summary window.

## Incident Report

6. Select the report icon found on top of the Copilot side panel to generate the Incident Report.

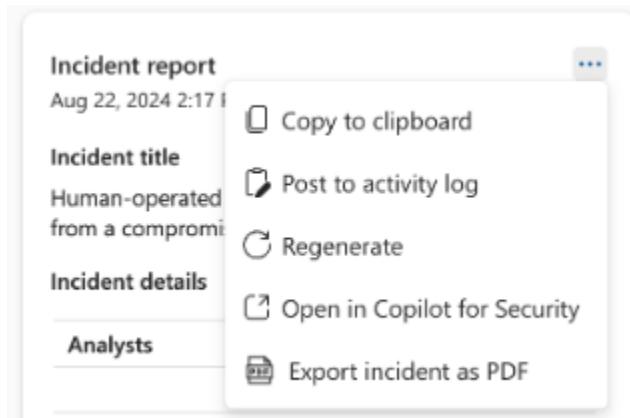
**Tip:** Alternatively, you can select the More actions ellipsis (...) on the incident page, then select Generate incident report.



7. Open the incident's activity log by clicking on the **More actions ellipsis (...)** and selecting **Activity log** on the incident pane.

**Tip:** Refer to the complexity of manually summarizing long activity logs into one report and the ability of Copilot to summarize this efficiently in the incident report.

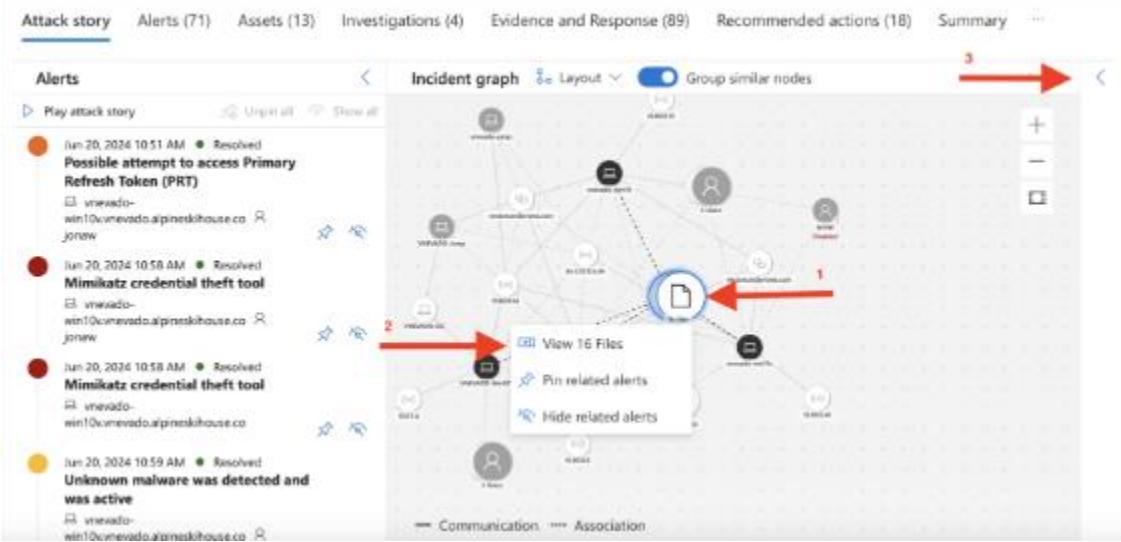
8. Once generated, the report can be copied to your preferred system or posted to the incident's activity log for record-keeping. By posting the report to the activity log, SOC teams can refer to the actions of an incident for future decision-making.



## File Analyzer

9. From the incident page, **Click Files (1) from the Attack Story Graph >Click View <nr> Files (2)> Expand Node Details (3).**

⌚ **Tip:** You can also choose a file to investigate in an alert page.



10. Select the file **Mimikatz.exe** file to investigate.

> [Back to incident details](#)

## 16 Files

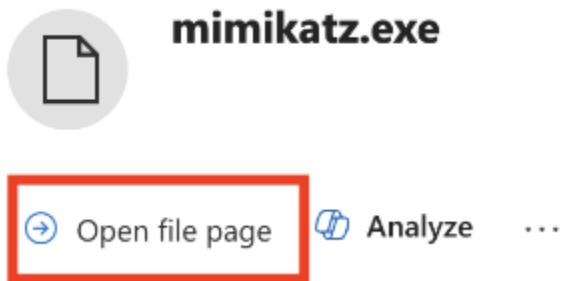
### Name

[notepad.exe](#)

[mimikatz.exe](#)

[mimikatz.exe](#)

11. Then select **Open File Page**. Copilot automatically generates an analysis upon opening a file page.



**Tip:** The file analysis results generated by Copilot typically include: Assessment of the file, detection name if malicious/unwanted, key file information, Highlights strings found, lists API calls used, and relevant certificate information.

## Script Analyzer

12. Within the incident page , select the PRT alert on the left pane, select the PowerShell script with the curl command line. Click **Analyze** to start the analysis.

**Tip:** This script that uses curl via PowerShell to access the PRT is a great example to see script analyzer in action.

A screenshot of the Microsoft Defender XDR interface. At the top, there are tabs for 'Attack story', 'Alerts (71)', 'Assets (13)', 'Investigations (4)', 'Evidence and Response (89)', 'Recommended actions (18)', 'Summary', and more. The 'Alerts' tab is selected. On the left, a list of alerts is shown, including: 'Jun 20, 2024 10:51 AM • Resolved Possible attempt to access Primary Refresh Token (PRT)' (orange), 'Jun 20, 2024 10:58 AM • Resolved Mimikatz credential theft tool' (red), 'Jun 20, 2024 10:58 AM • Resolved Mimikatz credential theft tool' (red), and 'Jun 20, 2024 10:59 AM • Resolved Unknown malware was detected and was active' (yellow). In the center, an 'Incident graph' shows various nodes and connections. On the right, a detailed view of the first alert is open. It shows a 'Command line' section with the text: '[2484] powershell.exe -Enc... Remote execution ...'. Below it is a 'Command line (decoded)' section with the text: 'powershell.exe -EncodedCommand YwB1AHIAbAAgAHYAZQbjAHQA'. A red box highlights the 'Analyze' button next to this text. Other buttons in this section include 'Details', 'Logs', and 'File'.

## Device Summary

13. Within the incident page, select the **Assets tab**  
14. Click **Devices** and click device **vnevado-win10r.vnevado.alpineskithouse.co** on the right.

Attack story   Alerts (71)   **Assets (13)**

All assets (13)

- Devices (8)**
- Users (5)
- Mailboxes (0)
- Apps (0)
- Cloud Resources (0)

⌚ **Tip:** This particular script that uses curl via PowerShell to access the PRT is a great example to see script analyzer in action.

vnevado-win10s

Medium Medium Criticality: Low

AlpineSkiHouse LiveResponse ModernWork - Full automation

Open device page Summarize Device value ...

15. Click **Open Device page**. Copilot automatically generates an analysis upon opening the device page.

⌚ **Tip:** Note the owner, software vulnerability and risky settings of the device.

## Activity 4: Intune Use Cases

### Estimated time to complete this activity

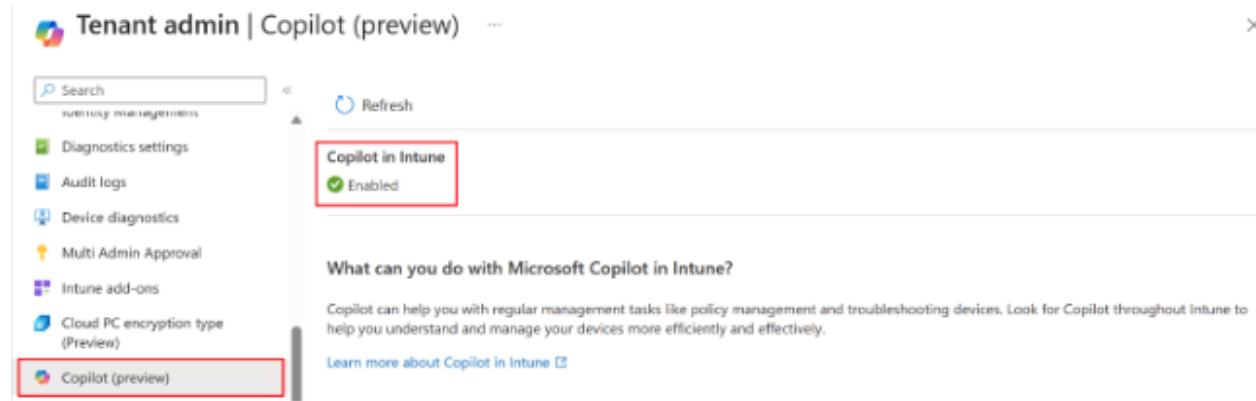
30 minutes

#### Exercise 1: Intune Policy Management with conflict analysis.

This exercise will give you a hands-on experience with the current Copilot for Security features embedded in the Intune portal. Copilot technology is assisting the device administrator in areas like managing policies and settings, understanding security posture, and troubleshooting of device issues.

**⚠️ Important Remark:** Before you can use the Copilot features in Intune, Microsoft Copilot for Security must be configured, and you must complete the first run tour in the [Microsoft Copilot for Security portal](#). For the setup tasks, see [Get started with Microsoft Copilot](#). Due to the nature of this lab, you will not be able to experience the "first run tour", but please familiarize yourself with below location to guide customers to the correct location to check that Copilot features has been enabled for Intune in their tenant.

Using your Alpine Skihouse account, access [Intune admin center](#) > **Tenant administration** > **Copilot**.

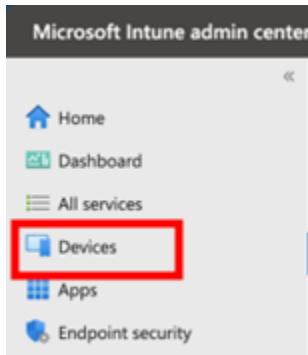


The case:

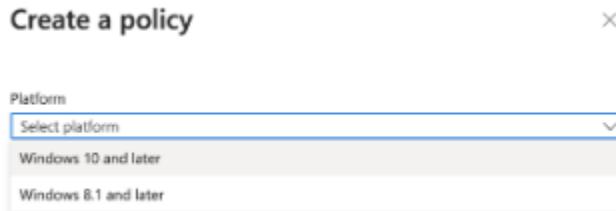
You are an IT admin responsible for ensuring that the Intune environment has the right set of policies required for device management in the environment. You are required to manage and maintain the current set of policies. There is a new task at hand to deliver a new Windows compliance policy. Hence – you need to quickly get up to speed on creating a Windows compliance policy, learn which settings to deliver, ensure there are no conflicts and figure out the recommended values for the various settings.



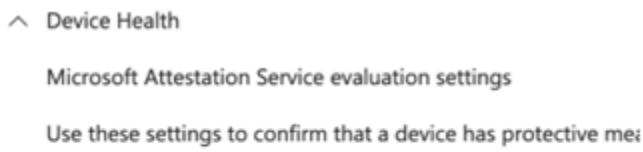
**⚠️ Important Remark:** Alpine Skihouse is a shared environment. Do not assign test-policies to any devices or users or groups, do not deploy your work to the tenant in the "review & create" guided wizard by using the "Create" button in the last step!



1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. Go to **Manage Devices** > **Compliance**
4. In the top menu, select “**+Create Policy**”
5. Select platform “**Windows 10 and later**” > click “**Create**” button



6. Provide a name for the policy (just some random characters - non PII data) > click “**Next**”
7. Unfold “Device Health” and select the Copilot icon right next to “BitLocker”



8. Copilot provides a description of the setting, as well as any relevant sources, supporting your work as you are defining Windows compliance settings for your organization.
9. But importantly, you need to know if this specific compliance setting has been configured in any other policies!

Tell me about Intune setting "BitLocker"

## Fetched Document Summary

The "BitLocker" setting in the "DeviceHealth" category for the "Windows 10/11 compliance policy" on the "Windows 10 and later" platform is related to the BitLocker Drive Encryption feature in Windows. BitLocker helps protect the data on the device's operating system volume against unauthorized access and offline attacks.

Here are some key points from the fetched documents:

- BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted

10. Click the "book symbol" to see suggested prompts in the guide and explore further.

Please note that the "BitLocker" setting in Intune is not required by default, meaning it can be configured based on the organization's security requirements.

Sources:

- [1]: Device Compliance settings for Windows 10/11 in Intune ↗
- [2]: BitLocker and policy settings compliance ↗
- [3]: BitLocker-encrypted Windows 10 device shows as Not compliant in Intune ↗
- [4]: BitLocker settings reference ↗

AI generated content may be incorrect. Check it for accuracy.  

How could this setting affect users?

Does Microsoft recommend any particular value for this setting? 

Generated by Copilot for Security ↗ Learn more ↗

11. Select "Has this setting been configured in any other policies?"

Prompt guide

Tell me about Intune setting "BitLocker"

Has this setting been configured in any other policies?

Does Microsoft recommend any particular value for this setting?

How could this setting affect users?

How could this setting affect security?

Does Microsoft recommend any particular value for this setting? 

12. Copilot helps you and finds **any potential conflicting policies** that includes the same settings.

Has this setting been configured in any other policies?

The 'BitLocker' setting, which is part of the 'DeviceHealth' category for the 'Windows 10/11 compliance policy' on the 'Windows 10 and later' platform, is indeed configured in one of your existing policies. Here are the details of the policy:

- \* **Policy Id:** 22fc6a93-3336-4fc1-ab09-73abc2eb5092
- \* **Policy Name:** Device Risk

13. Just for good measure, you ask Copilot for Microsoft's recommendations for the setting you are configuring – **select “Does Microsoft recommend any particular value for this setting”** at the suggested prompts right next to the “book” icon.

Does Microsoft recommend any particular value for this setting?

Based on the fetched documents, the setting "BitLocker" under the "DeviceHealth" category for the "Windows 10/11 compliance policy" on the "Windows 10 and later" platform is not explicitly discussed. However, there are some general recommendations and practices related to BitLocker settings in the context of device compliance and security.

- In the context of device health, BitLocker is often used to encrypt

(Feel free to test out the other suggested prompts, before you continue the lab exercises)

**⚠ Important Remark:** Remember to NOT deploy your work to the tenant, **exit out** e.g. click "Devices Overview" in the path-menu – then select "OK" in the pop-up! (thank you)

Home > Devices | Overview > Windows | Compliance >

## Windows 10/11 compliance policy

Windows 10 and later

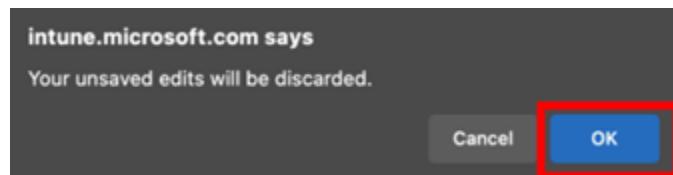
Basics    **Compliance settings**    Actions for noncomp

Custom Compliance

Device Health

Microsoft Attestation Service evaluation settings

Use these settings to confirm that a device has protective measures



## Exercise 2: Summarize Existing Policies & Assess their Impact to users & Security

You are a new IT admin that is tasked with reviewing and delivering a security policy for your environment encompassing BitLocker, ASR and more. You have inherited the role from another

admin and was informed that some policies have already been created. You need to be able to summarize the existing policy, and learn of its impact to users and security, prior to creating new ones or editing existing ones.

1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. Go to **Manage Devices** > **Configuration**
4. Select the “**Enhanced Ant phishing**” configuration policy
5. Select “Summarize with Copilot” to easily understand the purpose and configuration of the policy.

Summarize this policy

The policy in question is named “Enhanced Antiphishing”. It has several settings configured, which are as follows:

1. **Automatic Data Collection (Windows Insiders only)**: This setting is enabled and it allows for automatic collection of website or app content when additional analysis is needed to help identify security threats. Please note that this setting is only available to Windows Insiders.
2. **Notify Malicious**: This setting is enabled and it configures Enhanced Phishing Protection notifications for malicious content.
3. **Notify Password Reuse**: This setting is enabled and it configures Enhanced Phishing Protection notifications for protecting passwords from reuse.
4. **Notify Unsafe App**: This setting is enabled and it configures Enhanced Phishing Protection notifications for protecting passwords typed into M365 Office applications, Notepad, and Wordpad.
5. **Service Enabled**: This setting is enabled and it enables Enhanced Phishing Protection in audit mode for Windows 11 H2.

Home > Devices | Configuration >

**Enhanced Antiphishing** Device configuration profile

Summarize with Copilot Delete

Device and user check-in status

Succeeded	Error	Conflict	Not applicable	In Progress
31	0	0	0	0

[View report](#)

Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

6. But – you obviously need to get a better understanding of the user impact from the settings inside the policy. As in the previous Intune exercise, have a look and try the suggested prompts next to the “book icon”.

Describe the impact of this policy on users

Describe the impact of this policy on security



7. (Graphics intentionally left out) – Please take a closer look at the Copilot results, try to compare the first couple of descriptions of settings in the “Summarize” assistance you got, tox the results from the other two suggested prompts – Copilot can certainly help you describing impact to the users and the security in a language you can easily convey to your colleagues.

### Exercise 3: Assistance to troubleshoot devices

Now you are a helpdesk admin tasked with troubleshooting devices in Intune. You are facing a situation where policies and apps are missing from one device but are showing up on another devices. You need to quickly understand more about the devices and compare them for apps and policies.

1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. In the Device overview, use the Search field and type: CPC-u123-MCMLHU
4. Click on the Device name itself

The screenshot shows the Intune Admin Center interface. The top navigation bar includes 'Home', 'Devices | Overview', and a user icon. Below this is a horizontal menu with 'Windows devices' selected. On the left, there's a sidebar with 'Device onboarding', 'Windows 365', 'Enrollment', 'Manage devices', and 'Configuration'. The main area has a search bar containing 'CPC-u123-MCMLHU'. A message at the top right says 'December 31st, 2024 marks the end of Microsoft Intune: Android management options instead. Learn more about it.' Below the search bar are 'Refresh', 'Export', 'Columns', and 'Bulk' buttons. A table displays device information:

Device name	Managed by	Ownership
CPC-u123-MCM	Intune	Corporate

5. To get a quick overview of the device itself, you can use Copilot for Security features, click “Explore with Copilot”.

**CPC-u123-MCMLHU** ...

Search X <> **Explore with Copilot** Sync Restart

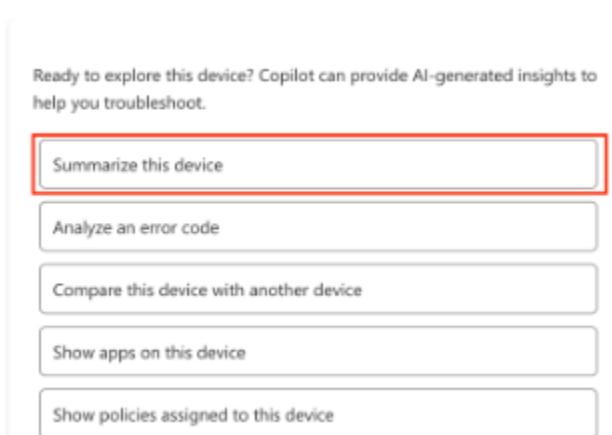
**Overview**

Manage Properties Monitor

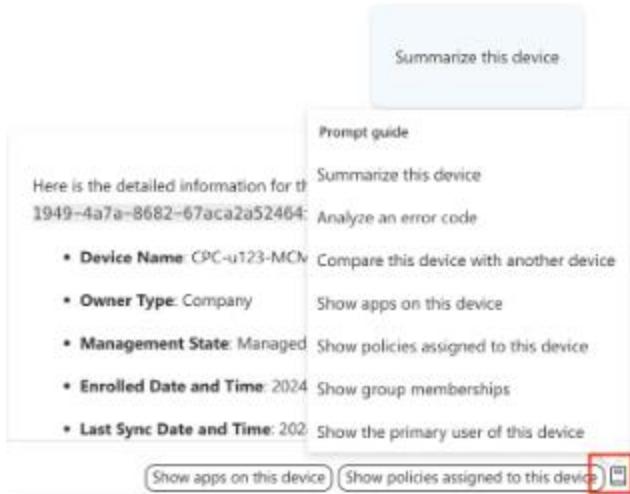
Reprovision: Completed

Device name : CPC-u123-MCMLHU

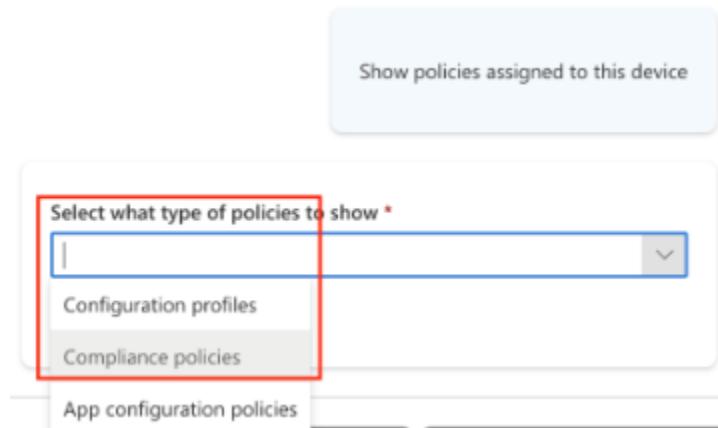
6. You are now presented with a range of options to explore the device with assistance. Choose "Summarize this device" to get a more in-depth presentation of key stats of the device.



7. Try to scroll down through all parts of the Summary, Copilot collects a lot of different insights about the device - saving you time to fetch them in different locations of the Intune portal. Next, try to click the "book icon" again, and you see a list of suggested prompts to continue your analysis of the device.



8. Obviously, you noticed, that the device was not compliant! – To understand why and get further details, select the suggested prompt “Show policies assigned to this device”.
9. A new menu pops up, select “Compliance policies”



10. You quickly get a complete list of the assigned policies and their status. Hence you can determine what made the device non-compliant and investigate in Intune why said policy has not applied or is not working on the device.

The device CPC-u123-MCMLHU with id 6d9d0270-2e61-4d5c-975a-fb570cbf5d2c has 2 compliance policies assigned to it. Here are the details:

PolicyId	PolicyName	PolicyStatus
c0f4911a-7ce6-4804-8563-677a2665d379	Default Device Compliance Policy	Compliant
22fc6a93-3336-4fc1-ab09-73abc2eb5092	Device Risk	Not compliant

The user associated with this device is u123@a.alpineskihouse.co. The device last contacted the server on 2024-08-28 20:59:55.000000.

**⚠ Important Remark:** Stay at current view after step 10 above, next exercise continues from same place.

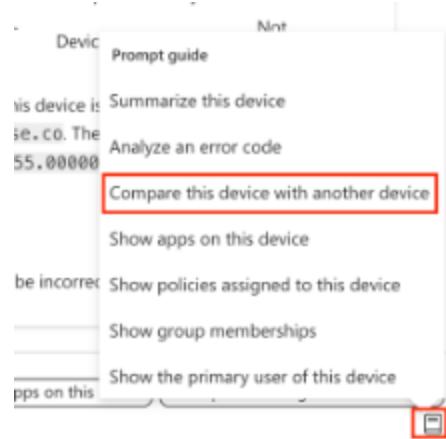
## Compare devices for troubleshooting

### Exercise 4: Compare devices for troubleshooting

A common troubleshooting scenario stems from users reporting e.g. missing apps, missing settings that gives a certain user experience etc. – the users experience the lack of something on their devices, or they realize their device is not configured in the same way as their peer's devices.

A quick way to try figure out why Device A is misconfigured or lacks some apps, is to compare it to a known correctly working device – Device B. Copilot for Security makes it much easier to compare two devices, instead of doing this by hand manually and collecting different stats about the devices at different places in the Intune portal.

1. Return to the screen from step 10 in the previous exercise and click the book icon.



2. Select "Compare this device with another device".

Select another device and what you want to compare

Device 2 \* ⓘ  
VNEVADO-Win10B

Comparison type \*  
Managed apps

Submit

3. For Device 2 fill in "VNEVADO-Win10B". Select the Comparison type drop down and select "Managed apps", hit Submit.
4. Try to revert to step 1 of this exercise and Compare devices again – this time select "Configuration Policies". Observe the rich details of differences.

The device CPC-u123-MCMLHU has a total of 4 managed apps, while the device VNEVADO-Win10B has a total of 6 managed apps.

The device CPC-u123-MCMLHU has no unique managed apps. However, the device VNEVADO-Win10B has 2 unique managed apps. Here are the details:

Application	Version	Resolved Intent	Installation Status
Microsoft 365 Apps for Windows 10 and later		requiredInstall	Installed
Microsoft Edge for Windows 10 and later	128.0.2739.54	requiredInstall	Installed

#### CPC-u123-MCMLHU differences:

PolicyName	PolicyStatus	UPN
Default Tamper Protection Policy	Succeeded	System account
Default Antivirus Policy	Succeeded	System account
Defender for Endpoint onboarding	Succeeded	u123@a.alpineskihouse.co

#### VNEVADO-Win10B differences:

PolicyName	PolicyStatus	UPN
Firefox extensions	Error	System account
Chrome extensions	Succeeded	System account
Purview Edge browser extension	Succeeded	System account
MDE Tamper Protection off	Succeeded	System account
MDAV not configured	Succeeded	System account
OneDrive	Succeeded	nestorw@vnevado.alpineskihouse.co

## Exercise 5: Analyzing error codes

As you were checking up on Irvin's Windows device, your eyes zoomed in on an error!! Copilot for Security to the rescue – follow the steps and try out how.

1. Jump back to the overview of the Windows devices.
2. Search for the device named "**ASH-IrvinS1**", in the list click the device name (in blue)

Enhanced Antiphishing	System account	Settings Catalog	Succeeded
<b>Firefox extensions</b>	System account	Device configuration	Error
Firewall Exception for Azure Bastion	u293@ash.alpineskihouse.co	Microsoft Defender Firewall Rules	Succeeded

3. On the new left-side menu, select "**Device Configuration**" and find the error

message at the “**Firefox extensions**” policy – BAM! Good thing your keen eyes found that error! Now click on the Firefox extensions to read out the error code.

The screenshot shows a sidebar with "Error code ↑↓" and a list containing "-2016281112". To the right, under "SOURCE PROFILES", there are two options: "Source Profile" and "Firefox extensions". Below this, under "ERROR CODE", it shows "0x87d1fde8".

4. You can use both error codes, the results will be the same when Copilot analyses them, copy one of them to you clip board.
5. Now jump back to the device “**ASH-IrvnS1**” overview page and invoke the “Explorer with Copilot” once more.
6. This time, from the different suggested prompts, select “Analyze an error code”
7. Paste in the error code and hit “Submit”

The screenshot shows a form with a button "Analyze an error code" above a text input field. The input field contains the text "-2016281112". Below the input field is a "Submit" button.

8. From the rich results you now know exactly what that error code means, and you can continue your work and correct the error.

The error code -2016281112 or 0x87D1FDE8 corresponds to “Remediation failed” [1]. This error can occur in different scenarios.

In the context of Microsoft Intune, this error can occur when you deploy a Managed Browser policy. Specifically, if you deploy the “Configure URLs that will be allowed or blocked in the Managed

9. This concludes the short exercise, above picture is only a snippet of the full response.

## Exercise 6: Advanced analyzing using KQL query

Unfortunately, the next frustrated user is already at your service desk. The user complains about the device's performance has decreased significantly and it's now too slow for day-to-day tasks. You need to figure out what processes might be causing this. Copilot provides a natural language to KQL feature embedded into the Intune console. This provides a very easy interface to perform highly sophisticated queries.

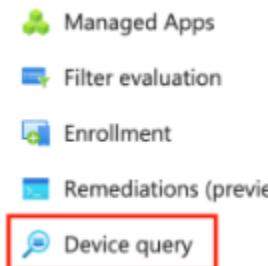
**⚠️ Important Remark:** Due to technical limitations of Alpine Skihouse, you will not be able to fully perform a KQL-based device query with a result returning from the device.

The Device Query feature using KQL leverages the Intune Advanced Analytics feature set. Please familiarize yourself with the prerequisites and limitations of running these types of queries by visiting the Microsoft Learn page on .

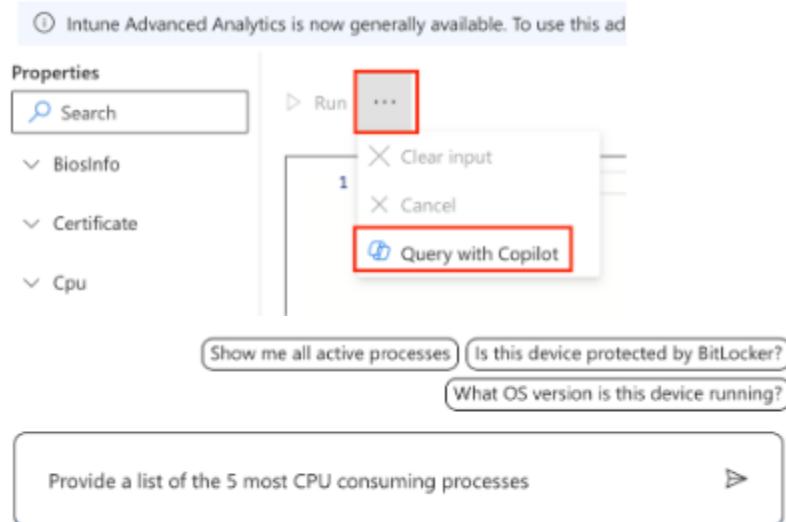
[What is Microsoft Intune Advanced Analytics - Microsoft Intune | Microsoft Learn](#)

<https://learn.microsoft.com/en-us/mem/analytics/device-query#supported-properties>

1. Head on back to the Windows Devices overview page in Intune.
2. Select the device named "**ASH-IrvinS1**"
3. In the left menu select "Device query"



4. Click the 3 small dots and select Query with Copilot
5. In the new pop-out menu, try to put in the natural language prompt: "Provide a list of the 5 most CPU consuming processes" and submit using the paper plane button.



- Copilot will build the KQL query and you get options to add it to your Device query window or – as we do now – select “Add and run”.

The screenshot shows a KQL query editor. It displays the following KQL code:

```
Process | summarize maxCpuUsage=max(SystemTimeMilliseconds) by ProcessName | top 5 by maxCpuUsage desc
```

Below the code are two buttons: 'Add to editor' and 'Add and run'. The 'Add and run' button is highlighted with a red box. There's also a link 'How was this query generated?' and a note 'AI generated content may be incorrect. Check it for accuracy.' with icons for copy and paste.

- Your beautiful KQL query is passed over and run. Please observe, that you will get a blank result / error message due to limitations of Alpine Skihouse.

**⚠️ Important Remark:** *Please observe, that you will get a blank result / error message due to limitations of Alpine Skihouse.*

Run Clear input Cancel Query with Copilot

```
1 // Generated by Copilot
2 Process | top 5 by WorkingSetSizeBytes desc
```

Example of a result, currently not possible in Alpine

Get started Results

Columns ▾

ProcessId	ProcessName	Path	CommandLine	CurrentWorkingSetSize	WorkingSetSize
3256	GlobalSecureAc...	C:\Program File...	"C:\Program Fil...	891949056	
4292	svchost.exe	C:\Windows\Sy...	C:\Windows\sy...	448966656	
8052	explorer.exe	C:\Windows\Ex...	C:\Windows\Ex...	247578624	
3504	MsSense.exe	C:\Program File...		234852352	
3576	MsMpEng.exe	C:\ProgramDat...		185671680	

8. Please observe, that even though you could ask Copilot to build some very technical KQL queries, there are limitations of the type of data that Intune can provide using Advanced Analytics features. For now, this Copilot feature will only provide KQL results that aligns with the data Advanced Analytics can provide. See more about this in the documentation (links provided in this exercise).

## Activity 5: Purview Use Cases

Estimated time to complete this activity

30 minutes

### Exercise 1: Data Loss Prevention

After investigating in the standalone experience, let's explore the embedded Data Loss Prevention experience. As a compliance administrator, the embedded environment makes it easier to get detailed data on generated alerts. This integration reduces the time spent understanding alerts by providing summaries, which is particularly helpful when learning a new product set. Even if you're familiar with alerts but new to Microsoft Purview Data Loss Prevention, these summarization features help bridge the knowledge gap. Let's see how to use these summarization capabilities.

1. Go to the new Purview portal at <https://purview.microsoft.com>) and sign in with your credentials.
2. Go to the Data Loss Prevention solution and navigate to the alerts queue.

Alert name	Severity	Status	Time detected	Insider risk severity
DLP policy match for document 'SiteSecurityServiceState.txt' on a device	High	Active	Aug 16, 2024 10:41 AM	High
DLP policy match for email with subject 'Document'	Low	Active	Aug 14, 2024 10:03 AM	High
DLP policy match for email with subject 'Document'	Low	Active	Aug 14, 2024 9:30 AM	High
DLP policy match for email with subject 'Testing Encryption Label'	Low	Active	Aug 7, 2024 4:29 AM	None
DLP policy match for email with subject 'Testing Encryption Label'	Medium	Active	Aug 7, 2024 4:29 AM	None

3. Choose the alert you want to review. In this case, let's choose “Alert: DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device”
4. Click on the “Get a summary from Security Copilot” option on the panel.

**Alerts**

If your role group permissions are restricted to a specific set of users, you'll only be able to view alerts for those users. [Learn more](#)

Did you know? You can now manage your DLP alerts in the Microsoft Defender portal! Alerts are automatically combined into incident investigation and remediation.

Export Refresh Set status

Filter Reset Filters

Time range: 7/19/2024-8/19/2024 User: Natasha.David\_0716@woodgrove.ms Alert status:

Alert name	Severity
DLP policy match for document 'SiteSecurityServiceState.txt' on a device	High
DLP policy match for document 'Teams SSN.docx' on a device	Low
DLP policy match for document 'Teams SSN.docx' on a device	High
DLP policy match for document 'google - software specifications - mtmprogprod...'	Low
DLP policy match for document 'google - software specifications - mtmprogprod...'	High
DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device	Low
DLP policy match for document 'google - software specifications - srsdocument...'	High
DLP policy match for document 'SSN.txt' on a device	Low
DLP policy match for document 'EOY Feedback.docx' on a device	High

**Alert: DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device**

**Details** **Events** **User activity summary**

**Summarize with Copilot**

**Alert ID**  
9c19b080-af20-71aa-1600-08dcaddb7dd0

**Alert status**  
Active

**Alert severity**  
High

**Time detected**  
Jul 26, 2024 6:31 PM

**Number of events**  
2

**DLP policy matched**  
AP - Block Cloud and USB

**Locations**  
Devices

**Users who performed the event**

Natasha David  
natasha.david\_0716@woodgrove.ms

**Assigned to**  
No one is assigned

## 5. Click View details at the same time at the bottom of the alert.

**Copilot**

Generating Alert summary...

Stop generating

**Alert ID**  
9c19b080-af20-71aa-1600-08dcaddb7dd0

**Alert status**  
Active

**Alert severity**  
High

**Time detected**  
Jul 26, 2024 6:31 PM

**Number of events**  
2

**DLP policy matched**  
AP - Block Cloud and USB

**Locations**  
Devices

**Users who performed the event**

Natasha David  
natasha.david\_0716@woodgrove.ms

**Assigned to**  
No one is assigned

## 6. Alert summary will be generated

## Alert: DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device

Details    Events    User activity summary

 Copilot

**Alert summary** ...  
Aug 19, 2024 1:10 PM

The high severity DLP alert with ID d19c19b080-af20-71aa-1600-08dcaddb7dd0 and Title "DLP policy (AP - Block Cloud and USB) matched for document (Cardholder Transaction Log.xlsx) in a device" was generated on July 27, 2024 01:28:00 (UTC). The alert is currently in "new" status and is associated with the user natasha.david\_0716@woodgrove.ms.

The policy responsible for this alert is named "AP - Block Cloud and USB" with Policy ID ed114f46-b224-434a-b4e5-7ab6fdd12b40. The rule that triggered the alert is "Block AP" with Rule ID 21975999-c5c9-4667-a975-e2d7ca0669a5. This is related to the workload Endpoint.

Additionally, Natasha.David\_0716@woodgrove.ms is marked as High risk level in Insider Risk Management.

AI-generated content may be incorrect. Check it for accuracy.  

7. Below is what the overall pane looks like for Full details. The Copilot summary condenses the necessary information into a few short paragraphs.

Alerts > DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device

## DLP policy match for document 'Cardholder Transaction Log.xlsx' on a device

■■■ High   ■ Active

[Overview](#)   [Events](#)

What happened

**Natasha David was involved in DLP policy violations.**

Between Jul 26, 2024 6:28 PM and Jul 26, 2024 6:29 PM DLP policy, "AP - Block Cloud and USB" was violated 2 times.

Name	User	Location
Sensitive info in 'Cardholder Transaction Log.xlsx' - File copied to removable USB device	Natasha David	Devices
Sensitive info in 'google - Information and cyber security policy - uow222145.pdf' - File copied...	Natasha David	Devices

**Actor details**

Users who performed the event  
Natasha David  
natasha.david\_0716@woodgrove.ms  
■■■ High  
[View user summary](#)

**Policy information**

Policy matched  
AP - Block Cloud and USB  
Rule matched  
Block AP  
Sensitive info types  
None  
Trainable classifiers  
None

**Alert information**

Alert ID  
9c19b080-a20-71aa-1600-08dcaddb7dd0  
Time detected  
Jul 26, 2024 6:31 PM  
Alert status  
Active  
Alert severity  
■■■ High

**Other alerts for this user**

Name	Severity
DLP policy match for document 'SiteSe...	■■■ High
DLP policy match for document 'Teams...	■■■ Low
DLP policy match for document 'Teams...	■■■ High

[See all alerts for this user](#)

**Manage alert**

[Assign](#)   [Management log](#)

Status  
Active

Assign to  
Start typing to find users

Comments  
Add comments about this alert

[Save](#)

8. You can use the three dots on the top right of the alert summary to copy the response to clipboard, regenerate, or open it in the standalone security copilot experience. The summary decreases the time needed to view the full View Details page.

Details    Events    User activity summary

---

 Copilot

**Alert summary**

Sep 25, 2024 5:34 PM

The high severity DLP alert with ID dl146bf2fa-7f...  
Title "DLP policy (U.S. Financial Data) matched fo...  
generated on September 14, 2024 17:00:00(UTC)  
and is associated with the user isbe@vnevado.al...

The email involved in this alert is isbe@vnevado.alpineskihouse.co.

The policy responsible for this alert is named "U.S. Financial Data" with Policy ID a93b9ed7-8c59-4bcd-b14b-77c586e2a48e. The rule that triggered the alert is "High volume of content detected U.S. Financial Data" with Rule ID 7ecfc508-7cba-47fe-b978-337fce162126. This is related to the workload Exchange.

AI-generated content may be incorrect. Check it for accuracy. 

## Exercise 2: Insider Risk Management

Similar to the DLP embedded experience, a compliance admin can use Insider Risk Management alerts to swiftly grasp potential issues by noting crucial user details like resignations, exfiltration activities, patterns, roles, and anomalies. This AI-driven summary aids security teams in focusing on critical evidence and investigation pathways. Follow these instructions to learn to use this summary feature, which helps newcomers to this technology quickly understand the product.

1. Go to the new Purview portal at <https://purview.microsoft.com>) and sign in with your credentials.
2. Go to the Insider Risk Management solution.
3. Go to your alerts queue by navigating to the alerts tab.

The screenshot shows the Microsoft Purview Insider Risk Management Alerts page. On the left, there's a sidebar with navigation links like Overview, Recommendations, Alerts (which is selected), Cases, Policies, Users, Reports, Forensic Evidence, Notice templates, Audit log, Adaptive protection (preview), Related solutions (Communication Compliance, Information Barriers), and Data Loss Prevention. The main area is titled 'Alerts' and contains a message about priority user groups. Below that is a 'Spotlight' section with a count of 1. There are buttons for 'Export' and 'Save'. A search bar at the top right shows '64 items' and 'Alerts tutorial'. The main table lists 64 alerts with columns for ID, Copilot, Users, Policy, Status, Spotlight, Alert severity, Time detected, Assigned to, and Case. One alert is highlighted: ID 627e940f, Copilot Lee Gu, User Ismat Bekarevich (OPS), Policy Data leaks quick policy..., Status Needs review, Alert severity Low, Time detected 2 days ago, Assigned to Unassigned.

- Choose the alert you want to review. For this example, please search “Isaiah” in the search bar and select. ID 86e52569.

The screenshot shows the same Microsoft Purview Insider Risk Management Alerts page, but with a search filter applied. The search bar at the top right now shows 'isaiah'. The results show 1 of 9 selected alerts. The table lists alerts for user 'Isaiah Langer' with various details. One alert is selected: ID 86e52569, Copilot Isaiah Langer, Policy Potential data theft - ..., Status Confirmed, Alert severity High, Time detected a year ago, Assigned to Unassigned, Case Case 034: Potential d... (status Active).

5. Click on the summarize alert button on the right from the Alerts page or through clicking into the alert.

The screenshot shows the Microsoft Purview Insider Risk Management interface. On the left, there's a navigation sidebar with 'Insider Risk Management' selected. The main area displays an alert titled '(86e52569) Potential data theft – Employee Departure'. The alert is marked as 'High Severity' with a risk score of 100/100. It was created on April 21, 2023 (UTC). The 'Cumulative exfiltration activities' section shows 348 events involving prioritized content. The 'Triggering event' was an HR connector importing a resignation date for the user. The 'User details' section identifies the user as 'Isaiah Langer' with the email 'isahl@woodgrove.ms'. The 'User alert history' shows no history. A red box highlights the 'Summarize' button in the top right corner.

6. Alert summary will be generated:

This screenshot shows the same alert page after generating a summary. The summary is located in the bottom right corner of the main alert card. It includes the alert ID, creation date, and a detailed description of the findings. The description states that the alert is a 'Potential high impact user' who accessed more content with prioritized sensitivity labels than 97% of other users. It also mentions that 140 other activities have the same risk score of 100/100. The summary concludes by stating the alert is in 'Confirmed' state and is being investigated under case 'Case 034: Potential data leak'. It also notes the user is considered high risk based on the following risk factors:

- User is a member of a priority user group from August 15, 2024 to August 16, 2024 (UTC) because they are part of the 'Sensitive Project Contoso Members' group.
- HR event: Employment end date was set on August 3, 2024 (UTC) with the resignation reason 'Leaving company'.
- Emails with attachments sent outside the organization on August 18, 2024 (UTC) - User is found to be sending 6 emails outside the organization.
- Sensitive SharePoint files accessed on August 10, 2024 (UTC) - User is found to be accessing 6 sensitive SharePoint files. The files contained 5 instances of sensitivity info, were shared on 1 SharePoint site, contained priority content, had 1 sensitivity label applied, and were accessed on 1 or more SharePoint sites with sensitivity label applied.

The summary also includes AI-generated content for accuracy and provides links to related actions like listing sequential activities or summarizing user activity.

7. In another process, if you were to go back to the previous page with all the alerts, you could click on a summary without clicking into the alert.

**Alerts**

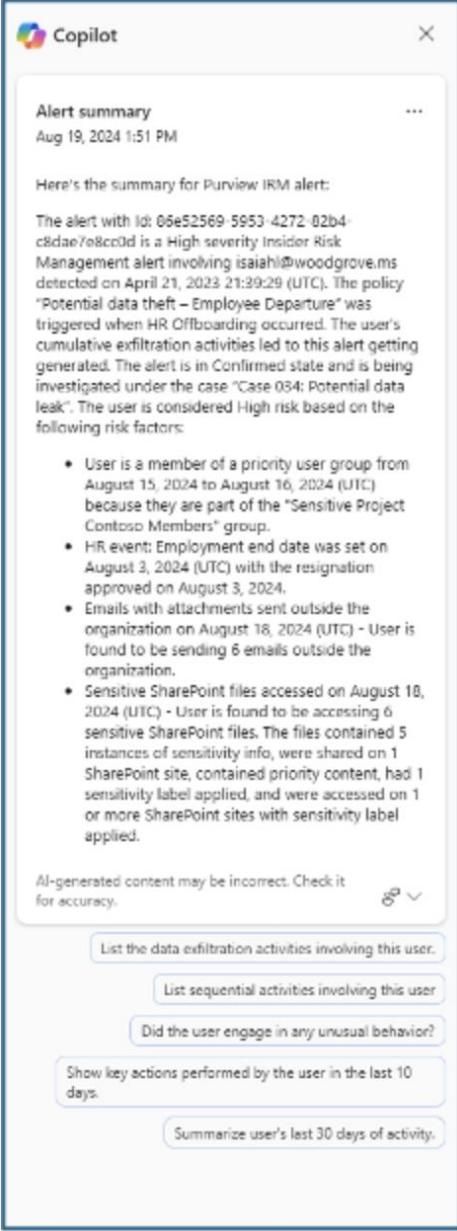
(1) Priority user groups are not currently supported for use with Admin Units. It is recommended to ensure that the reviewers of a priority user group are not restricted to specific admin units. [Learn more about admin units.](#) [X](#)

 [Summarize with Copilot](#) [Export](#) [Dismiss alerts](#) [Assign](#) 1 of 9 selected [Alerts tutorial](#)  [Customize columns](#)

Filter set: [Save](#)

<input type="checkbox"/> ID	<input type="checkbox"/> Copilot	<input type="checkbox"/> Users	<input type="checkbox"/> Policy	<input type="checkbox"/> Status	<input type="checkbox"/> Spotlight	<input type="checkbox"/> Alert severity	<input type="checkbox"/> Time detected	<input type="checkbox"/> Assigned to	<input type="checkbox"/> Case	<input type="checkbox"/> Case status
<input type="checkbox"/> 38fc08ab	<input checked="" type="checkbox"/>	Isaiah Langer	Data leaks quick polic...	<span>● Confirmed</span>	<span>■■■ High</span>	4 months ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> e65be3bc	<input checked="" type="checkbox"/>	Isaiah Langer	Data leaks quick polic...	<span>● Confirmed</span>	<span>■■■ High</span>	5 months ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> c32904d3	<input checked="" type="checkbox"/>	Isaiah Langer	Data leaks quick polic...	<span>● Confirmed</span>	<span>■■■ High</span>	6 months ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> 6a85b9c5	<input checked="" type="checkbox"/>	Isaiah Langer	Data leaks quick polic...	<span>● Confirmed</span>	<span>■■■ High</span>	7 months ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> 87a21518	<input checked="" type="checkbox"/>	Isaiah Langer	Data leaks quick polic...	<span>● Confirmed</span>	<span>■■■ High</span>	a year ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> af7ad1cb	<input checked="" type="checkbox"/>	Isaiah Langer	Project TNT - Alert	<span>● Confirmed</span>	<span>■■■ High</span>	a year ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> beb2847f	<input checked="" type="checkbox"/>	Isaiah Langer	Adaptive Protection p...	<span>● Confirmed</span>	<span>■■■ Medium</span>	a year ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input type="checkbox"/> 5ef4f3eb	<input checked="" type="checkbox"/>	Isaiah Langer	Project Obsidian	<span>● Confirmed</span>	<span>■■■ High</span>	a year ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	
<input checked="" type="checkbox"/> 86e52569	<input checked="" type="checkbox"/>	Isaiah Langer	Potential data theft – ...	<span>● Confirmed</span>	<span>■■■ High</span>	a year ago	Unassigned	Case 034: Potential d...	<span>● Active</span>	

8. This will then take away the need to go into each individual alert to get a summary.



The screenshot shows a Copilot alert summary window. At the top left is the Copilot logo and the word "Copilot". At the top right is a close button ("X"). Below the title, it says "Alert summary" and "Aug 19, 2024 1:51 PM". There are three dots at the top right of the main content area. The main content area contains the following text:

Here's the summary for Purview IRM alert:

The alert with Id: 06e52569-5953-4272-02b4-c8dae/08cc0d is a High severity Insider Risk Management alert involving isaiah@woodgrove.ms detected on April 21, 2023 21:39:29 (UTC). The policy "Potential data theft - Employee Departure" was triggered when HR Offboarding occurred. The user's cumulative exfiltration activities led to this alert getting generated. The alert is in Confirmed state and is being investigated under the case "Case 034: Potential data leak". The user is considered High risk based on the following risk factors:

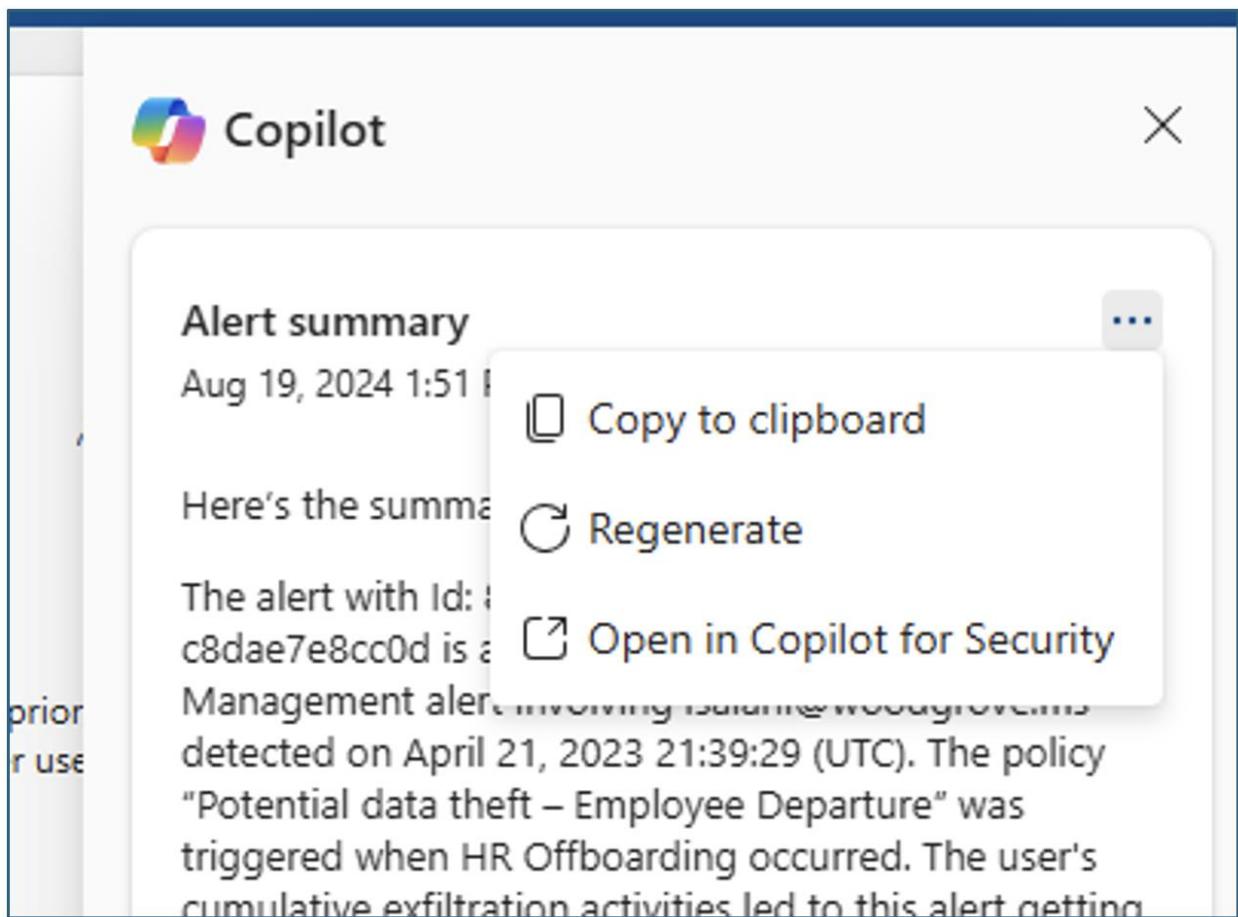
- User is a member of a priority user group from August 15, 2024 to August 16, 2024 (UTC) because they are part of the "Sensitive Project Contoso Members" group.
- HR event: Employment end date was set on August 3, 2024 (UTC) with the resignation approved on August 3, 2024.
- Emails with attachments sent outside the organization on August 18, 2024 (UTC) - User is found to be sending 6 emails outside the organization.
- Sensitive SharePoint files accessed on August 18, 2024 (UTC) - User is found to be accessing 6 sensitive SharePoint files. The files contained 5 instances of sensitivity info, were shared on 1 SharePoint site, contained priority content, had 1 sensitivity label applied, and were accessed on 1 or more SharePoint sites with sensitivity label applied.

AI-generated content may be incorrect. Check it for accuracy.  

Below the main content are several buttons:

- List the data exfiltration activities involving this user.
- List sequential activities involving this user.
- Did the user engage in any unusual behavior?
- Show key actions performed by the user in the last 10 days.
- Summarize user's last 30 days of activity.

9. You can use the three dots on the top right of the alert summary to copy the response to clipboard, regenerate or open it in the standalone security copilot experience.



10. You can click on any of the recommended prompts to get more data. In this case, select "Summarize user's last 30 days of activity."

Summarize user's last 30 days of activity.

Document was last saved: Just now  
User activity summary ...  
Aug 19, 2024 1:54 PM

Microsoft Purview Insider Risk Management found the following activities involving isaiah@woodgrove.ms from July 20, 2024 20:53:36(UTC) to August 19, 2024 00:00:00(UTC):

- Exfiltration: User is found to be sending emails with attachments outside the organization 6 times on August 18, 2024 23:59:59(UTC). The emails contained a total of 6 emails and were sent to 1 recipient.
- Access: User is found to be accessing sensitive SharePoint files 6 times on August 18, 2024 23:59:59(UTC). The files contained 5 instances of sensitivity info, were found on 1 SharePoint site, contained priority content, had 1 sensitivity label applied, and were found on 1 or more SharePoint sites with sensitivity labels applied.
- Deletion: User is found to be deleting SharePoint files 16 times on August 16, 2024 23:59:59(UTC). The files contained 1 instance of sensitivity info, were found on 1 SharePoint site, and contained priority content.

To get a detailed view of isaiah@woodgrove.ms's activities: [View all activity](#).

AI-generated content may be incorrect. Check it for accuracy.  ▾

List the data exfiltration activities involving this user.

List sequential activities involving this user.

Did the user engage in any unusual behavior?

Show key actions performed by the user in the last 10 days.

1 (Risk score)  
449  
4  
Priority count  
814 activities  
Show all previous

Most of the follow-up questions for insider risk management are here in the embedded scenario here (follow-up prompts)

## Activity 6: Entra Use Cases

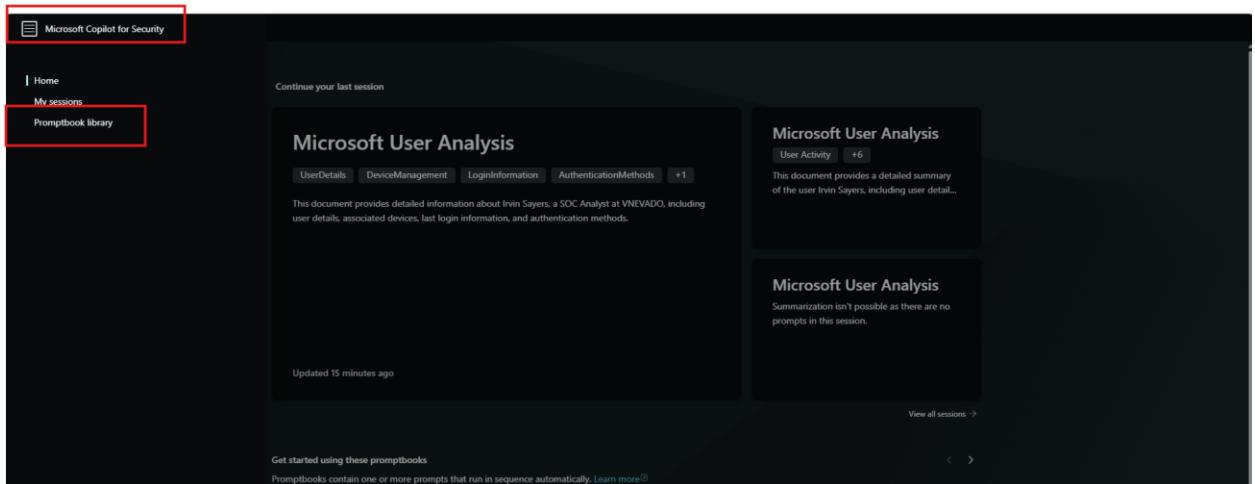
Estimated time to complete this activity

30 minutes

### Exercise 1: Run Promptbook Microsoft User Analysis

For this exercise let's go back to the standalone experience

1. Open your browser, and go to the Copilot for <https://securitycopilot.microsoft.com/>
2. Select the  home menu in the left corner
3. Navigate to Promptbook library



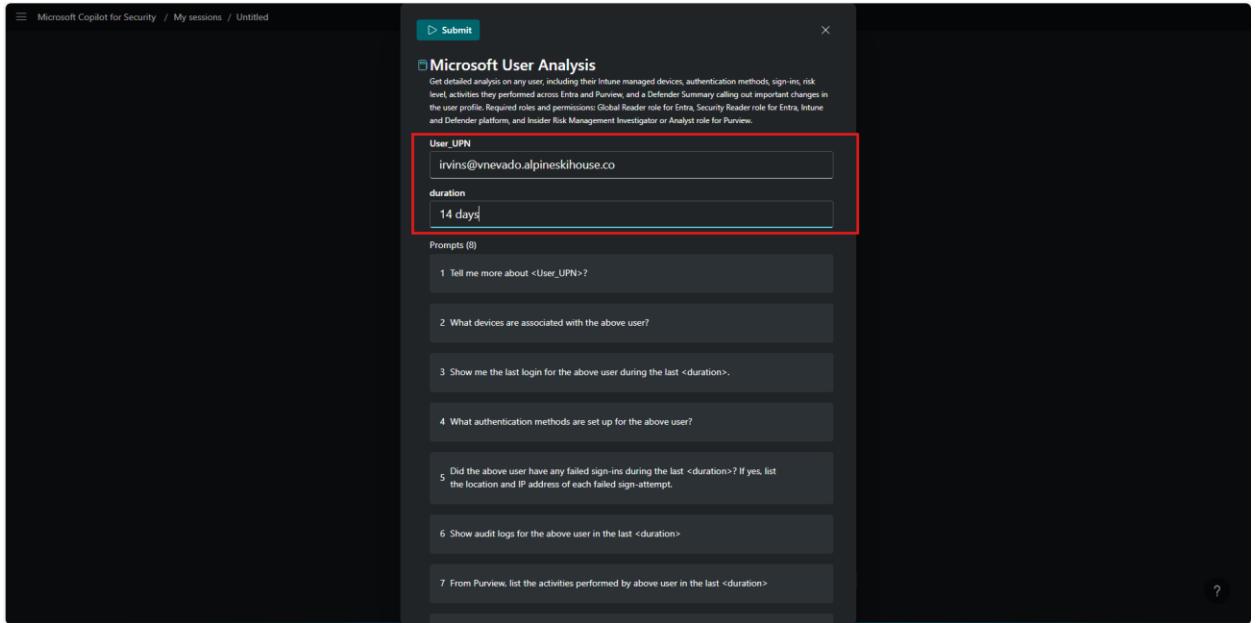
4. Click on the Microsoft tab and then click on “Microsoft User Analysis” Promptbook

The screenshot shows the Microsoft Copilot for Security interface with the "Promptbook library" tab selected. A red box highlights the "Microsoft" tab in the top navigation bar. Another red box highlights the "Microsoft User Analysis" promptbook in the list, which is described as providing detailed analysis on any user, including their Intune managed devices, authentication methods, sign-ins, risk level, activities they performed across Entra and Purview, and a Defender Summary calling out important changes in the user profile. Required roles and permissions include Global Reader role for Entra, Security Reader role for Entra, Intune and Defender platform, and Insider Risk Management Investigator or Analyst role for Purview.

5. Click on “Start a new Session”

The screenshot shows the Microsoft Copilot for Security interface with the "Promptbook library" tab selected. A red box highlights the "Microsoft" tab in the top navigation bar. A larger red box highlights the "Start new session" button for the "Microsoft User Analysis" promptbook. The session details are shown in a modal window, including the prompt name, description, and a list of 8 prompts. The first prompt is: "Tell me more about <User\_UPN>?"

6. Field the details with “[irvins@vnevado.alpineskihouse.co](mailto:irvins@vnevado.alpineskihouse.co)” and 14 days respectively



## 7. Go through the results

The screenshot shows the results of the Microsoft User Analysis. The first result is 'User Details for irvins@nevado.alpineskihouse.co' with a summary of user information:

- Name: Irvin Sayers
- Title: SOC Analyst
- Email: irvins@nevado.alpineskihouse.co
- User Principal Name (UPN): irvins@nevado.alpineskihouse.co
- User ID: 100070e4-61f1-4ee8-9fb0-02ab4edc4d8
- Company: NEVADO
- Department: Operations
- Account Enabled: Yes
- Created Date: 2023-12-20T11:11:32Z

To verify this information in the Microsoft Entra portal, you can navigate to the [User Management page](#) and search for this user.

This summary includes 1 item.

The second result is 'Devices Associated with Irvin Sayers (irvins@nevado.alpineskihouse.co)' showing 2 Intune managed devices. Below is the detailed information for each device:

Device Name	Platform	Last Seen
Irvin Sayers' Laptop	Windows 11 Pro	Now 1:55 PM
Irvin Sayers' Phone	Android	Now 1:55 PM

[Export to Excel](#)

## Exercise 2: Risky users summarization

1. Go to the Entra portal (<https://entra.microsoft.com/>) and sign in with your credentials.
2. Scroll down on the left hand menu and expand "Protection" and then click on "Risky activities"

The screenshot shows the Microsoft Security Center interface. The left sidebar is titled 'Favorites' and includes sections for Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, and Show more. Under the 'Protection' section, there are sub-options: Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities (which is highlighted with a red box), and Learn & support.

The main content area is titled 'Security | Risky users'. It features a search bar and various navigation and filter options at the top. A message encourages setting up automatic risk remediation. Below this is a table listing 'Risky users' with columns for User ID, Risk state, Status, and Last updated. The table shows several users, including Lee Gu, who is listed as 'Confirmed compromised'.

User	Risk state	Status	Last updated
u2406	At risk	30/10/2024, 17:04:20	...
u3135	At risk	30/10/2024, 00:31:25	...
Lee Gu	Confirmed compromised	29/10/2024, 21:29:03	...
u2762	At risk	26/10/2024, 01:31:40	...
u2707	At risk	25/10/2024, 17:44:14	...
u2678	At risk	25/10/2024, 00:49:38	...
u2034	At risk	24/10/2024, 04:02:29	...
u2935	At risk	23/10/2024, 19:59:16	...
u2014	At risk	22/10/2024, 18:33:11	...
Jonathan Wolcott	At risk	19/10/2024, 10:41:40	...
u1393	At risk	19/10/2024, 04:37:09	...
u562	At risk	17/10/2024, 20:54:59	...
u1105	At risk	17/10/2024, 04:47:59	...
u542	At risk	17/10/2024, 02:02:08	...

3. Click on user "Lee Gu"

## Risky User Details

X

 Reset password  Confirm user compromised  Confirm user safe  Dismiss user risk  Block user | ...

 Summarize Basic info Recent risky sign-ins Detections not linked to a sign-in Risk history

### Summary by Copilot

Generated by Copilot

- User Lee Gu has three recent risky activities, all with High risk level.
- The risk detection types are Admin confirmed user compromised, Microsoft Entra threat intelligence, Anonymous IP address, Password spray, and Malicious IP address.
- Admin confirmed user compromised denotes reported compromise by a human administrator and elevates the overall user risk to high accordingly.
- Microsoft Entra threat intelligence is a risk detection type without a description.
- Anonymous IP address indicates sign-ins from an anonymous IP address (for example, Tor browser or anonymous VPN).
- Password spray is a risk detection type triggered when a password spray attack has been successfully performed.
- Malicious IP address indicates sign-in from a malicious IP address based on high failure rates because of invalid credentials received from the IP address or other IP reputation sources.
- Risky sign-in 1 (RequestId: 4d33d597-3949-4467-8894-1dbb07dd8400, CorrelationId: d3ffdb75-6fa1-4928-9f67-22732daecb00) with High risk level occurred for Application null and Resource null. The sign-in IP was 185.220.101.15 and location was Hamburg, Hamburg DE. The IP, ASN, Location, Browser Id, and Device Id were unfamiliar to the user. There was no MFA for this sign-in.
- Risky sign-in 2 (RequestId: 0d263ce9-0a80-4699-9577-661a22257200, CorrelationId: ffe6b08e-f34a-44b3-a471-e34651c1c46a) with High risk level occurred on 2024-09-09T13:37:08 UTC for Application null and Resource OfficeHome. The sign-in IP was 109.70.100.66 and location was Wieden, Wien AT. The IP, ASN, Location, Browser Id, and Device Id were unfamiliar to the user. There was no MFA for this sign-in.

AI-generated content may be incorrect  

4. Copilot will return an analysis of what happened, and how best to mitigate and remedy the situation.