

## 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 .....	29
Activity 5: Purview Use Cases .....	44
Exercise 1: Data Loss Prevention.....	44
Exercise 2: Insider Risk Management.....	48
Activity 6: Entra Use Cases .....	55
Exercise 1: Sign-logs Investigation.....	55
Exercise 2: Risky users summarization .....	57

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

## Exercise 1: Copilot for Security Standalone Experience

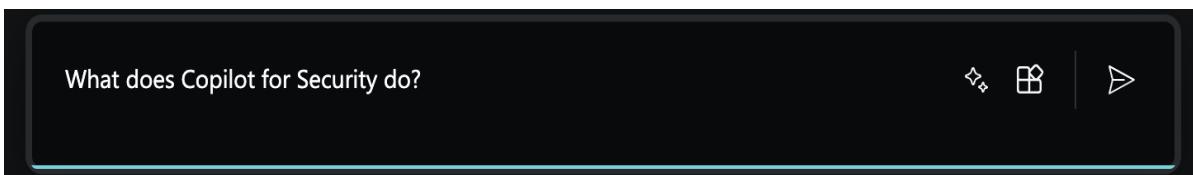
In this exercise, you will explore the Copilot for Security Standalone Experience. You will learn how to navigate the portal, manage plugins, and utilize various features to enhance your security operations. This hands-on activity will help you become familiar with the capabilities of Copilot for Security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

The screenshot shows a dark-themed interface for Microsoft Copilot for Security. At the top, there is a search bar with the placeholder text "What does Copilot for Security do?". Below the search bar, a list of completed steps is displayed. The first step, "3 steps completed 40 seconds", has a green checkmark icon and a dropdown arrow. An orange arrow points from the text "3 steps completed" towards this icon. The second step, "Chose Microsoft Documentation 8 seconds", also has a green checkmark icon and is highlighted with a red rectangular box. The third step, "Searched documentation 19 seconds", and the fourth step, "Prepared your response 13 seconds", both have green checkmark icons but are not highlighted.

- 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 >

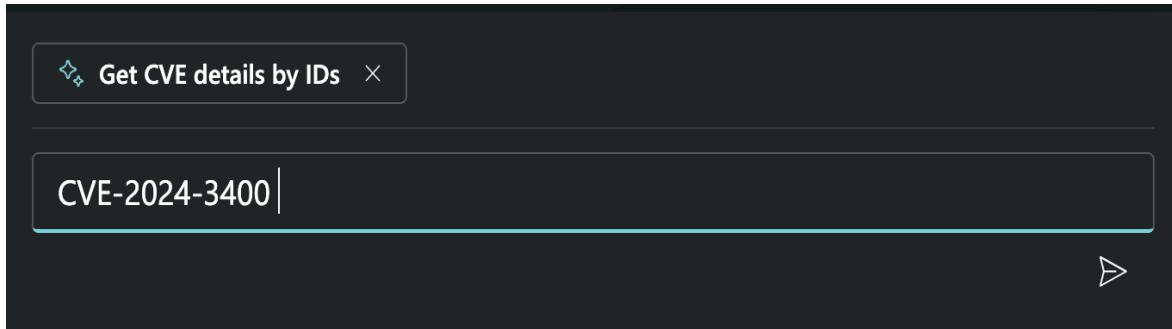
Capabilities are based on the plugins you have set up.

**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.

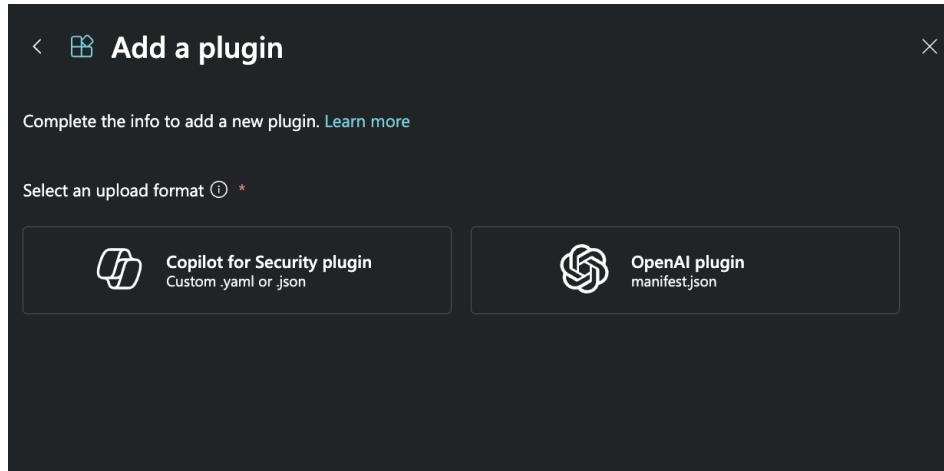
The screenshot shows the 'Manage sources' interface with the 'Plugins' tab selected. A search bar and filter buttons for 'All (29)', 'On (10)', and 'Off (19)' are at the top. Below is a list of Microsoft plugins:

Plugin	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.*

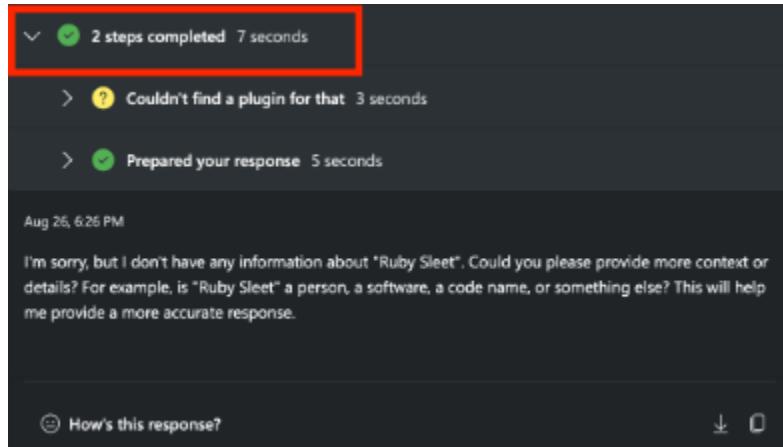


### Effective vs non effective prompts

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:



<https://aka.ms/>

### 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 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

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**.

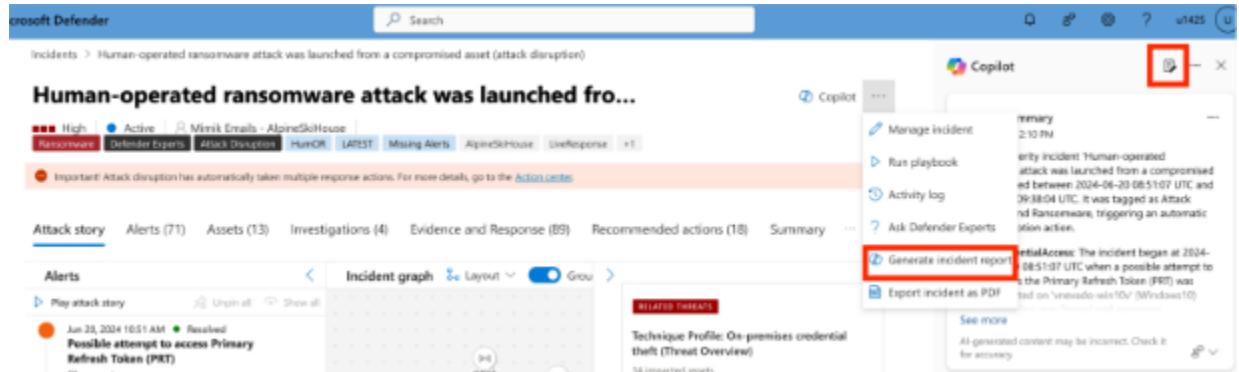
**Tip:** Each card contains information about the recommended action, including the entity where the action needs to be applied and why the action is recommended. The cards also emphasize when a recommended action was done.

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.

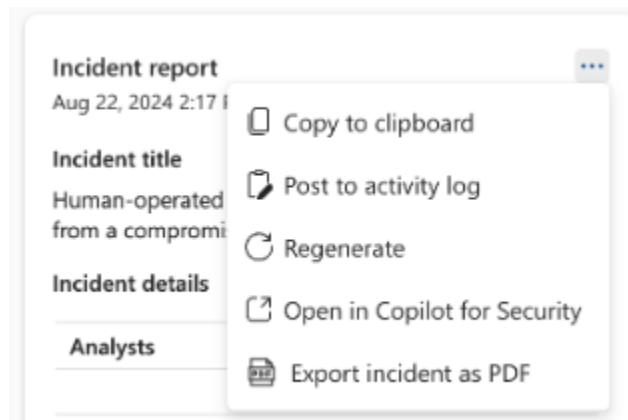
 **Tip:** Alternatively, you can select the More actions ellipsis (...) on the incident page, then select Generate incident report.



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.

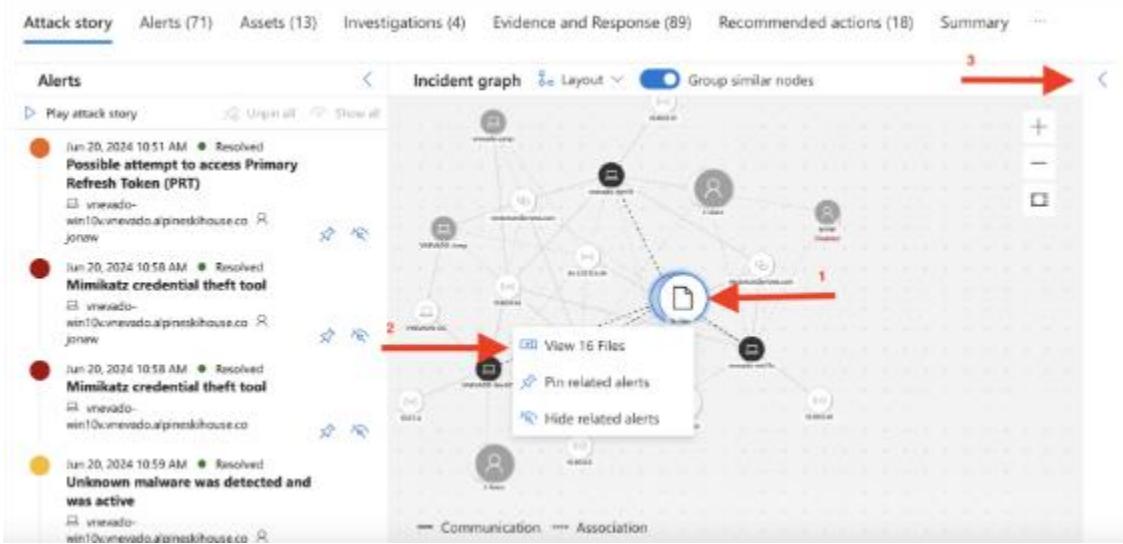
8. Once generated, the report can be copied to your preferred system or posted to the incident's activity log for record-keeping. By posting the report to the activity log, SOC teams can refer to the actions of an incident for future decision-making.



## 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.



The screenshot shows the Microsoft Defender XDR interface. On the left, there's a list of alerts with details like date, status, and description. The main area is the 'Incident graph' which displays various nodes (hosts, files, users) connected by lines representing communication or association. A specific file node is highlighted with a blue border and a red arrow labeled '1' points to it. A context menu is open over this node with three options: 'View 16 Files' (also highlighted with a red arrow labeled '2'), 'Pin related alerts', and 'Hide related alerts'. Another red arrow labeled '3' points to the top right corner of the graph area, likely indicating a zoom or filter function.

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

> [Back to incident details](#)

## 16 Files

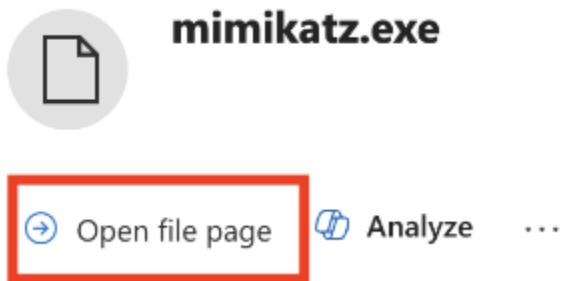
### Name

[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 incident page. The top navigation bar includes 'Attack story', 'Alerts (71)', 'Assets (13)', 'Investigations (4)', 'Evidence and Response (89)', 'Recommended actions (18)', 'Summary', and more. The 'Alerts' tab is selected, displaying a list of alerts: '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). On the right, there's an 'Incident graph' with nodes and connections, and a detailed view of the first alert. Under 'Command line', it shows '[2484] powershell.exe -Enc... Remote execution ...' with a decoded command line: 'powershell.exe -EncodedCommand YwB1AHIAbAAgAHYAZQbjAHQA'. A red box highlights the 'Analyze' button for this command line.

## 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

### Prerequisites

- Copilot for Security must be enabled.
- Microsoft Intune must be configured for all the supported Operating systems with a few policies created and devices enrolled.
- Intune Suite Add-on licenses must be assigned and very specifically the Device query experience must be set up correctly and working.

### Introduction

This document walks the readers through a set of scenarios that can be executed as part of the prompt-a-thon exercise.

### Core capabilities

- Policy Management
- Troubleshooting
- Copilot into Device query
- SoC integration

The above capabilities enable the IT admins to gain value from the Copilot in Intune experience.

### Scenarios (Embedded)

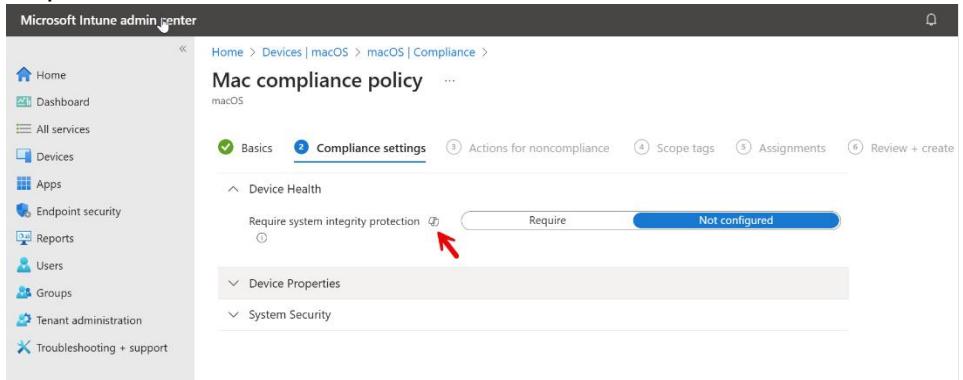
#### *Policy management*

- 1- Corey is an IT admin responsible for ensuring that the Intune environment has the right set of device management policies to meet her organization's business requirements.

Corey has been asked to ensure that macOS devices meet a base level of security before they are able to access corporate resources. To do this, Corey knows that she needs to create a new macOS compliance policy but is unsure of which settings to configure.

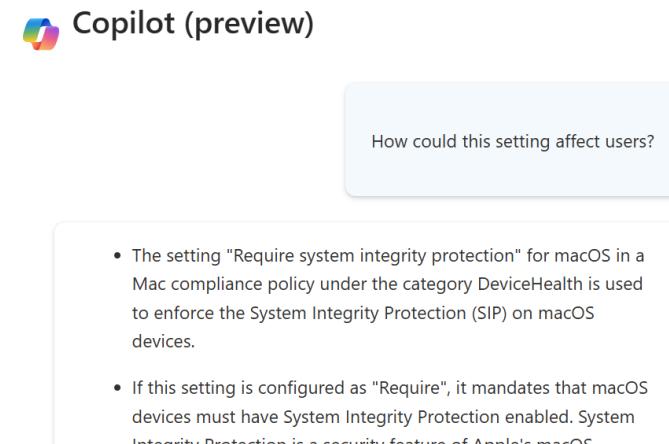
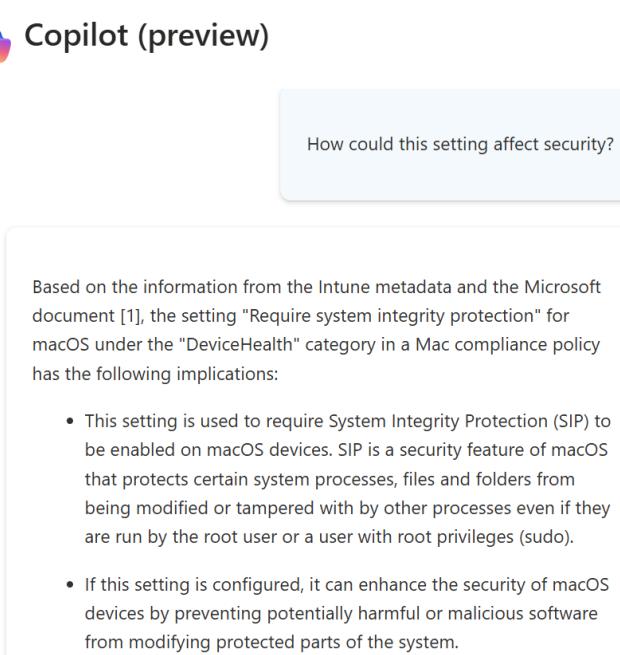
Corey can use Copilot to quickly obtain the information that she needs to:

- a. learn which settings to configure.
- b. Determine the recommended values for the various settings.
- c. Ensure that there are no conflicts with existing policies.

Prompt	Expected outcome
<p>Tell me about Intune setting "Require system integrity protection"</p>	<p>Corey goes to Devices and selects macOS. She then clicks Compliance, where she can click “+Create Policy” and then clicks “Create”.</p> <p>After providing a policy name and description, she clicks “Next” to check the “Compliance Settings”. Expanding “Device Health” she sees the setting “Require system Integrity protection” and clicks the Copilot button next to it:</p>  <p>A description of the setting is presented, as well as any relevant sources, supporting Corey as she is defining macOS compliance settings for their organization:</p>

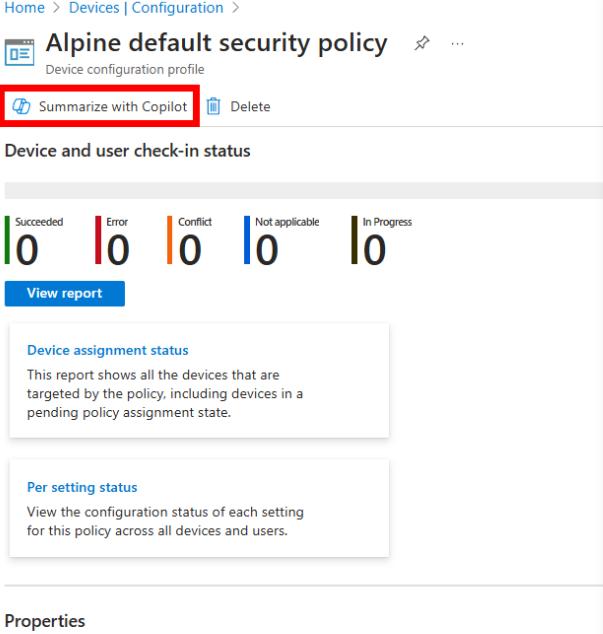
	<p> Copilot (preview) <span style="float: right;">X</span></p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>Tell me about Intune setting "Require system integrity protection"</p> <p>Based on the information from the Intune metadata and the fetched documents:</p> <ul style="list-style-type: none"> <li>• <b>Require system integrity protection:</b> This setting is used to enforce the System Integrity Protection on macOS devices. When this setting is configured, it requires macOS devices to have System Integrity Protection enabled. System Integrity Protection is a security feature of Apple's macOS operating system. When enabled, it helps protect the system by limiting the root account and preventing certain system processes from being terminated [1]. This setting is not mandatory and can be configured based on the organization's security requirements.</li> </ul> <p>Please note that this information is based on the local setting definition and the Microsoft document [1]. For the most accurate and up-to-date information, please refer to the official Microsoft documentation.</p> <p>Sources:</p> <p>[1]: Device Compliance settings for macOS settings in Intune <a href="#">🔗</a></p> <p>AI generated content may be incorrect. Check it for accuracy. <a href="#">🔗</a> <a href="#">🔗</a></p> <p style="text-align: center;"><a href="#">How could this setting affect users?</a> <a href="#">Does Microsoft recommend any particular value for this setting? </a></p> <p>Generated by Copilot for Security <a href="#">🔗</a> <a href="#">Learn more </a></p> </div>
Has this setting been configured in any other policies?	<p>Corey clicks on the book symbol in the bottom right of the window to see the suggested prompts in the guide to explore further:</p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>Please note that this information is based on the local setting definition and the Microsoft Prompt guide information,</p> <p>Sources:</p> <p>[1]: Device Compliance settings for macOS settings in Intune <a href="#">🔗</a> Has this setting been configured in any other policies?</p> <p>AI generated content may be incorrect. Does Microsoft recommend any particular value for this setting?</p> <p style="margin-left: 20px;"><a href="#">How could this setting affect users?</a></p> <p style="margin-left: 20px;"><a href="#">How could this setting affect security?</a></p> <p style="text-align: center;"><a href="#">Does Microsoft recommend any particular value for this setting? </a></p> <p>Generated by Copilot for Security <a href="#">🔗</a> <a href="#">Learn more </a></p> </div> <p>Corey selects the “Has this setting been configured in any other policies?” to avoid potential conflicts before deploying this new compliance policy.</p>

	<p> Copilot (preview) <span style="float: right;">X</span></p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>Has this setting been configured in any other policies?</p> </div> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>The setting "Require system integrity protection" for macOS under the policy type 'ComplianceMac' and setting category 'DeviceHealth' has been configured in one policy in your account.</p> <p><b>Setting Details:</b></p> <ul style="list-style-type: none"> <li>• <b>Setting Name:</b> Require system integrity protection</li> <li>• <b>Platform:</b> macOS</li> <li>• <b>Policy Type:</b> ComplianceMac</li> <li>• <b>Setting Category:</b> DeviceHealth</li> <li>• <b>Setting ID:</b> ComplianceMac_DeviceHealth_complianceSystemIntegrityProtectionName_10868</li> </ul> <p><b>Policies Configured:</b></p> <ul style="list-style-type: none"> <li>• <b>Policy Name:</b> Alpine Ski House macOS Compliance - Integrity Protection</li> </ul> </div>
Does Microsoft recommend any particular value for this setting?	<p>Corey tries this prompt to learn what Microsoft's recommendations are for the setting she is configuring.</p> <p> Copilot (preview) <span style="float: right;">X</span></p> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>Does Microsoft recommend any particular value for this setting?</p> </div> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px; margin-top: 10px;"> <p>Based on the information from the Intune metadata, the setting "Require system integrity protection" for macOS under the Mac compliance policy is not required. This setting is used to require System integrity protection to be enabled on the device.</p> <p>However, Microsoft does not provide a specific recommendation for this setting. The choice between "Not configured" and "Require" would depend on the specific security needs and policies of your organization. If your organization prioritizes a high level of security and wants to</p> </div>
How could this setting affect users?	Corey is also considerate of user experience and how compliance settings might affect it, so she tries this prompt to learn about the

	<p>effects of the setting to users. She will use this information to optimize the setting value according to their organizations use cases.</p>  <ul style="list-style-type: none"> <li>The setting "Require system integrity protection" for macOS in a Mac compliance policy under the category DeviceHealth is used to enforce the System Integrity Protection (SIP) on macOS devices.</li> <li>If this setting is configured as "Require", it mandates that macOS devices must have System Integrity Protection enabled. System Integrity Protection is a security feature of Apple's macOS</li> </ul>
How could this setting affect security?	<p>Lastly, Corey needs to work with the security team to ensure configuration is up to the organization's standards, so she uses this prompt to learn about the effects this setting could have on the device's security posture and ensure they respect the organization's security guidelines.</p>  <p>Based on the information from the Intune metadata and the Microsoft document [1], the setting "Require system integrity protection" for macOS under the "DeviceHealth" category in a Mac compliance policy has the following implications:</p> <ul style="list-style-type: none"> <li>This setting is used to require System Integrity Protection (SIP) to be enabled on macOS devices. SIP is a security feature of macOS that protects certain system processes, files and folders from being modified or tampered with by other processes even if they are run by the root user or a user with root privileges (sudo).</li> <li>If this setting is configured, it can enhance the security of macOS devices by preventing potentially harmful or malicious software from modifying protected parts of the system.</li> </ul>

- 2- Joy is a new IT admin that is tasked with reviewing and delivering a security policy for her environment encompassing BitLocker, ASR and more. She inherited the role from another admin and was informed that some policies have already been

created. She needs to be able to summarize the existing policy, and learn of its impact on users and security, prior to creating new ones or editing existing ones.

Prompt	Expected outcome
Summarize this policy	<p>Joy navigates to the already existing policy by clicking on <i>Devices &gt; Configuration</i> and then selecting the <i>Alpine default security policy</i>, and then clicks on the ‘Summarize with Copilot’ button.</p> <p>A summary of the policy and the included settings and their values should be displayed, allowing Joy to easily determine what this policy is meant to configure.</p>  <p>Copilot (preview)</p> <p>Summarize this policy</p> <p><b>Policy Summary: Alpine Default Security Policy</b></p> <p><b>Policy Settings:</b></p> <ol style="list-style-type: none"> <li><b>Allow Cortana Above Lock:</b> Allows interaction with Cortana using speech while the system is locked. Current setting: Allow.</li> <li><b>Allow Toasts:</b> Allows toast notifications above the device lock screen. Current setting: Allow.</li> <li><b>Allow Adding Non-Microsoft Accounts Manually:</b> Allows adding non-MSA email accounts through UI/UX-based methods. Current setting: Allow.</li> <li><b>Disable the Display Control Panel (User):</b> Disables the Display Control Panel. Current setting: Disabled.</li> <li><b>Hide Settings tab (User):</b> Removes the Settings tab from Display in Control Panel. Current setting: Disabled.</li> <li><b>Allow Warning For Other Disk Encryption:</b> Disables all UI</li> </ol>
Describe the impact of this policy on users	<p>Joy clicks on the book icon to see the available prompts for this policy. Joy selects ‘Describe the impact of this policy on users’ to understand what impact the settings and their values contained within this policy will have specifically on user experience when deployed.</p>

	<p>Home &gt; Devices   Configuration &gt;</p> <h2>Alpine default security policy</h2> <p>Device configuration profile</p> <p><a href="#">Summarize with Copilot</a> <a href="#">Delete</a></p> <p>Device and user check-in status</p> <p><a href="#">View report</a></p> <p><b>Device assignment status</b> This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.</p> <p><b>Per setting status</b> View the configuration status of each setting for this policy across all devices and users.</p> <p><b>Properties</b></p> <p><a href="#">Basics</a> <a href="#">Edit</a></p> <table border="1"> <tbody> <tr> <td>Name</td> <td>Alpine default security policy</td> </tr> <tr> <td>Description</td> <td>This is basic security policy for Alpi</td> </tr> <tr> <td>Platform</td> <td>Windows</td> </tr> </tbody> </table> <p><a href="#">Summarize this policy</a> <a href="#">Describe the impact of this policy on security</a> <a href="#">Copilot (preview)</a></p>	Name	Alpine default security policy	Description	This is basic security policy for Alpi	Platform	Windows	<p>Copilot (preview)</p> <p>Describe the impact of this policy on users</p> <p><b>User Impact of Implementing the Alpine Default Security Policy</b></p> <p>Implementing the Alpine Default Security Policy will have several impacts on users:</p> <ol style="list-style-type: none"> <li><b>Allow Cortana Above Lock:</b> Users will be able to interact with Cortana using speech while the system is locked, enhancing convenience but potentially raising privacy concerns.</li> <li><b>Allow Toasts:</b> Users will receive toast notifications above the lock screen, ensuring they do not miss important alerts even when the device is locked.</li> <li><b>Allow Adding Non-Microsoft Accounts Manually:</b> Users can add non-Microsoft email accounts through UI/UX-based methods, providing flexibility in email management.</li> <li><b>Disable the Display Control Panel (User):</b> Users will be unable to access the Display Control Panel, which could limit their ability to adjust display settings.</li> <li><b>Hide Settings tab (User):</b> The Settings tab will be removed from the ribbon.</li> </ol> <p>Generated by Copilot for Security <a href="#">Learn more</a></p>
Name	Alpine default security policy							
Description	This is basic security policy for Alpi							
Platform	Windows							
Describe the impact of this policy on security	Joy again clicks on the book icon and this time selects 'Describe the impact of this policy on security' to understand what impact the settings and the values contained within this policy will have on the security of devices when deployed.							

**Alpine default security policy**

Device configuration profile

Summarize with Copilot Delete

Device and user check-in status

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

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

**Per setting status**  
View the configuration status of each setting for this policy across all devices and users.

**Properties**

**Basics** Edit

Name	Alpine default security policy
Description	This is basic security policy for Alpine
Platform	Windows

09

**Copilot (preview)**

Describe the impact of this policy on security

**Security Impact of Implementing the Alpine Default Security Policy**

Implementing the Alpine Default Security Policy will have several significant impacts on security:

- Allow Cortana Above Lock:** Allowing Cortana interactions while the system is locked can pose a security risk by potentially exposing sensitive information or enabling unauthorized actions through voice commands.
- Allow Toasts:** Allowing toast notifications above the lock screen can expose sensitive information when the device is locked, which could be exploited in shared or public environments.
- Allow Adding Non-Microsoft Accounts Manually:** Permitting the addition of non-Microsoft accounts can introduce security risks by allowing potentially malicious accounts to be added, which might not be fully vetted by Microsoft accounts.
- Disable the Display Control Panel Enhances:** Control Panel enhances security by preventing users from changing system settings that could compromise security.

Summarize this policy | Describe the impact of this policy on users | Generated by Copilot for Security | Learn more

## Troubleshooting

- 1- Aaron is a helpdesk admin tasked with troubleshooting devices in Intune. Aaron is facing a situation where a user is able to successfully elevate and install a particular app on one device, but not on another. He suspects that Endpoint Privilege Manager (EPM) policies are missing from one device (FIELD-340181) but are applied successfully on another device (FIELD-694635). He needs to quickly understand more about the devices and compare their policies to confirm his suspicions.

Prompt	Expected outcome
Summarize this device	Aaron navigates to the device (FIELD-340181) that is experiencing issues and selects the 'Explore device' button to see the available prompts, and then selects 'Summarize this device'.  Copilot will present information about this device, such as its hardware information, the groups that the device is a member of, the device compliance state, and, if applicable, the reason for non-compliance.

The screenshot shows the Microsoft Intune Device Overview page for a device named 'FIELD-340181'. The left sidebar lists various management and monitoring options. A red box highlights the 'Explore with Copilot' button at the top right of the main content area. The right side displays the 'Copilot (preview)' interface, which includes a summary of the device's essentials (device name, management name, ownership, serial number, phone number, and manufacturer), a table for device actions status (Action: No data, Status: No data), and a list of AI-generated insights such as 'Summarize this device', 'Analyze an error code', 'Compare this device with another device', 'Show apps on this device', 'Show policies assigned to this device', 'Show group memberships', and 'Show the primary user of this device'. A note at the bottom states: 'Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.'

Home > Devices | Windows > Windows | Windows devices >

**FIELD-340181** ...

Search << Explore with Copilot Retire X

**Overview**

- Manage
  - Properties
- Monitor
  - Hardware
  - Discovered apps
  - Device compliance
  - Device configuration
  - App configuration
  - Local admin password
  - Recovery keys
  - User experience
  - Device diagnostics
  - Group membership
  - Managed Apps
  - Filter evaluation
  - Enrollment

^ Essentials

Device name  
FIELD-340181

Management name  
u2544\_Windows\_10/14/2024\_10:35 AM

Ownership  
Corporate

Serial number  
8198-8892-3078-5257-6508-3464-82

Phone number  
---

Device manufacturer  
Microsoft Corporation

Device actions status

Action	Status
No data	No data

Copilot (preview)

Ready to explore this device? Copilot can provide AI-generated insights to help you troubleshoot.

Summarize this device

Analyze an error code

Compare this device with another device

Show apps on this device

Show policies assigned to this device

Show group memberships

Show the primary user of this device

Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.

View prompts

Generated by Copilot for Security Learn more

	 <h2>Copilot (preview)</h2> <div style="text-align: right;">X</div> <div style="text-align: right; border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <a href="#">Summarize this device</a> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <h3>Device Information Summary</h3> <ul style="list-style-type: none"> <li>• <b>Intune Device ID:</b> <a href="#">2feb9045-856a-4625-91a4-26cd56b08ab2</a></li> <li>• <b>Azure AD Device ID:</b> <a href="#">7cd83681-aea7-469d-be38-c4d0973ea357</a></li> <li>• <b>Device Name:</b> FIELD-340181</li> <li>• <b>Owner Type:</b> Company</li> <li>• <b>Management State:</b> Managed</li> <li>• <b>Operating System:</b> Windows 10.0.22631.4317</li> <li>• <b>Compliance State:</b> Compliant</li> <li>• <b>Last Sync Date:</b> 2024-10-14T20:54:13.7426472Z</li> <li>• <b>Enrolled Date:</b> 2024-10-11T01:31:34.5983176Z</li> <li>• <b>Device Type:</b> WindowsRT</li> </ul> <div style="text-align: center; margin-top: 10px;"> <a href="#">Show apps on this device</a> <a href="#">Show policies assigned to this device</a>            Generated by Copilot for Security  <a href="#">Learn more</a>  </div> </div>
Compare this device with another device	<p>Aaron has been provided with another device (FIELD-694635) that can successfully elevate the app. To assist with troubleshooting, Aaron asks Copilot to compare the device with the missing policies with the device that has the policies successfully applied.</p> <p>To do so, Aaron clicks on the book icon and selects ‘Compare this device with another device’. Aaron supplies the name of the device and selects ‘Configuration profiles’ as the comparison type.</p> <p>Copilot will compare policies applied on both devices and highlight any differences.</p>



## Copilot (preview)

Compare this device with another device

Select another device and what you want to compare

Device 2 \* ⓘ

FIELD-694635

Comparison type \*

Configuration profiles

Submit

The device **FIELD-340181** has a total of 17 distinct device configuration policies, generating 28 status reports. The device **FIELD-694635** has a total of 19 distinct device configuration policies, generating 31 status reports. This is because some policies may be assigned to multiple users, resulting in multiple status reports for a single policy.

- **FIELD-340181** has 0 different configuration policies.
- **FIELD-694635** has 2 different configuration policies.

### Differences in Configuration Policies

FIELD-694635

Policy Name	Policy Status	User Principal Name
Intune EPM Rules - PowerToys	Succeeded	<a href="#">u2544@ash.alpineskihouse.co</a>
Intune EPM Settings	Succeeded	<a href="#">u2544@ash.alpineskihouse.co</a>

No differences were found for the device **FIELD-340181**.

#### Sources:

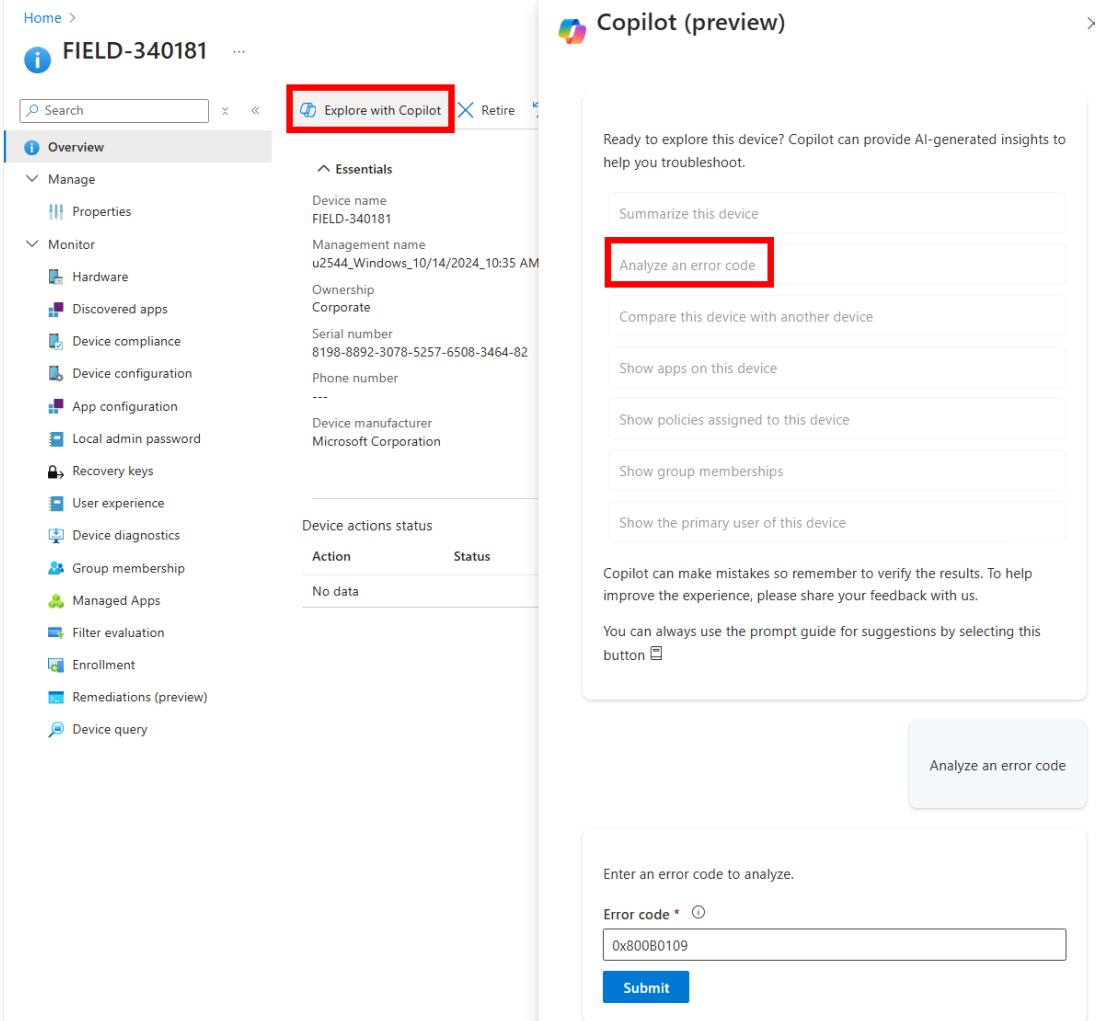
[Microsoft Intune](#) ⓘ

[Microsoft Intune](#) ⓘ

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

	With this information, Aaron can see that the device is indeed missing the required policies, which he can then easily remediate.
--	-----------------------------------------------------------------------------------------------------------------------------------

- 2- Whilst troubleshooting, Aaron has also come across some error codes that he does not know the meaning of and decides to ask Copilot what they correlate to.

Prompt	Expected outcome
Analyze an error code (0x800B0109)	<p>Aaron has found an error code whilst troubleshooting the device but is not sure what it correlates to and decides to ask Copilot.</p> <p>Aaron clicks on the ‘Explore with Copilot’ button while viewing a device and selects ‘Analyze an error code’. He then supplies the error code in box provided (0x800B0109) and clicks ‘Submit’.</p> <p>Copilot will provide an explanation of the error code to Aaron to assist with troubleshooting and resolution.</p> 

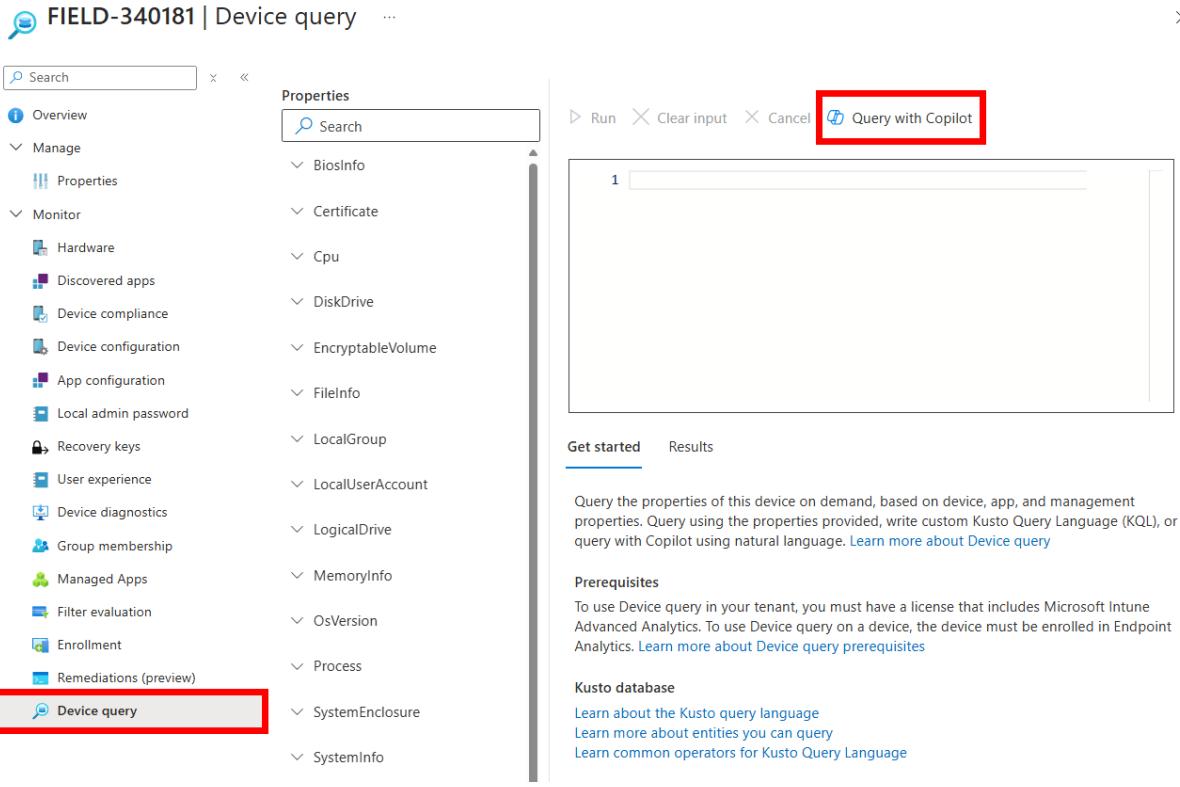
	<p> Copilot (preview) <span style="float: right;">X</span></p> <p>Enter an error code to analyze.</p> <p>Error code * ⓘ</p> <input type="text" value="0x800B0109"/> <p><span style="background-color: #f0f0f0; padding: 2px 5px; border-radius: 5px;">Submit</span></p> <p>The error code 0x800B0109 indicates a certificate error, specifically that the certificate chain is not trusted because it does not have a Microsoft Root CA signed root. This issue can occur in various scenarios, such as when Windows Server Update Services (WSUS) fails to sync with Microsoft on a Windows Server 2008 R2 server. The error is logged in the SoftwareDistribution.log file as:</p> <pre style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> 1 The given certificate chain has not Microsoft Root CA signed root (800B0109) 2 The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel 3 </pre> <p>To resolve this issue, you need to ensure that the WSUS application on the server is SHA2-compliant. Microsoft changed the signing process to use SHA2 only. You can fix this problem by downloading and installing the Update for Windows Server 2008 R2 for x64-based Systems (KB4484071) released on November 12, 2019 [1].</p> <p>For further details, you can refer to the Microsoft documentation provided.</p> <p>Sources:</p> <p><a href="#">WSUS doesn't sync with Microsoft on Windows Server 2008 R2 servers because of a certificate error</a> ⓘ</p> <p>AI generated content may be incorrect. Check it for accuracy. <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px;">✖️</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px;">🔍</span></p> <p style="text-align: right;"><span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 10px;">Analyze an error code</span> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;">Copilot for Security</span> ⓘ <a href="#">Learn more</a> ⓘ</p>
Analyze an error code	(Optional) Aaron has collated additional error codes that he has encountered during his day-to-day duties and decides to also ask Copilot if it can help determine what a few of them mean: <ul style="list-style-type: none"> <li>• 0x87D136B9</li> <li>• 0x87D136B8</li> </ul>

- 0x87D136B7
- 0x87D136B6
- 0x87D136B5
- 0x87D136B4
- 0x87D136B3
- 0x87D136B2

The screenshot shows the Copilot (preview) interface. At the top, there's a navigation bar with a Copilot icon and the text "Copilot (preview)" next to it, followed by a close button (X). Below the navigation bar is a large rectangular input field containing the text "Enter an error code to analyze." Inside this field, there's a form for entering an error code. The form has a label "Error code \* ⓘ" and a text input field containing "0x87D136B8". Below the input field is a "Submit" button. To the right of the input field is a button labeled "Analyze an error code". Below the input field, the text "The error code 0x87D136B8 corresponds to a 'Mismatched certificates' issue. This error indicates that there is a discrepancy between the certificates being used, which can cause problems with device configuration or profile installation [1]. Sources: Errors returned by iOS/iPadOS devices" is displayed. At the bottom of the interface, there's a note "AI generated content may be incorrect. Check it for accuracy." followed by a "Copy" icon and a "Rewrite" icon. At the very bottom, there's another "Analyze an error code" button.

### *Copilot into Device query*

- 1- Ravi is an Intune admin tasked with leveraging the new Intune suite device query platform for gaining on-demand information about the state of the devices. He needs to leverage Kusto Query Language (KQL) in order to use the feature, however he is new to KQL and needs guidance.

Prompt	Expected outcome
<p>What are the top 10 processes using the most memory on this device?</p>	<p>Ravi hears from an end user that their device's performance has decreased significantly and is getting too slow.</p> <p>Ravi needs to know what processes might be causing this, so he selects the device (FIELD-340181) in the Microsoft Intune admin center and goes to the 'Device query' tab. He selects 'Query with Copilot' to ask Copilot to write him the appropriate KQL query. He then clicks 'Add and Run' to see the results of the query.</p>  <p>Home &gt; Devices   Overview &gt; Windows   Windows devices &gt; FIELD-340181</p> <p>FIELD-340181   Device query</p> <p>Properties</p> <p>Get started Results</p> <p>Query the properties of this device on demand, based on device, app, and management properties. Query using the properties provided, write custom Kusto Query Language (KQL), or query with Copilot using natural language. <a href="#">Learn more about Device query</a></p> <p>Prerequisites</p> <p>To use Device query in your tenant, you must have a license that includes Microsoft Intune Advanced Analytics. To use Device query on a device, the device must be enrolled in Endpoint Analytics. <a href="#">Learn more about Device query prerequisites</a></p> <p>Kusto database</p> <p><a href="#">Learn about the Kusto query language</a>  <a href="#">Learn more about entities you can query</a>  <a href="#">Learn common operators for Kusto Query Language</a></p>



## Copilot (preview)

What are the top 10 processes using the most memory on this device?

Here is a KQL query that can help you get that information.

KQL query

```
Process | order by WorkingSetSizeBytes desc | take 10
```

Add to editor

Add and run

How was this query generated?

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

The query is automatically added to the editor and executed.

▶ Run ✎ Clear input ✖ Cancel ⚡ Query with Copilot

```
1 // Generated by Copilot
2 Process | order by WorkingSetSizeBytes desc | tail
```

Get started Results

ProcessId	ProcessName	Path	CommandLine	Curr
3236	MsMpEng.exe	C:\ProgramDat...		
7068	MsSense.exe	C:\Program File...		
9364	Microsoft.Mana...	C:\Program File...	"C:\Program Fil...	

Ravi can use the scroll bars to see the additional columns and rows returned.

Show me the top 20 running processes on this device and exclude wmicprvse	Ravi also wants to understand the top processes running on the device to determine if that may also be contributing to the reported poor performance of the user's device.  Ravi also wants to ensure that the process for WMI Provider Host is excluded. Ravi again clicks on the 'Query with Copilot' button and in the query box, he asks Copilot to "Show me the top 20 running processes on this device and exclude wmicprvse".  Once Copilot has returned the KQL query, Ravi selects 'Add and run' to automatically execute the query.
---------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Copilot (preview)

Show me the top 20 running processes on this device and exclude wmicprvse

Here is a KQL query that can help you get that information.

KQL query

```
Process | where ProcessName != 'wmicprvse' | top 20 by ElapsedTimeMilliseconds desc
```

Add to editor **Add and run**

How was this query generated?

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

---

Show me all active processes Is this device protected by bitlocker? What OS version is this device running?

▶ Run Clear input Cancel Query with Copilot

```
1 ///// Generated by Copilot
2 ///Process | order by WorkingSetSizeBytes desc
3 //
4 //// Generated by Copilot
5 //Process | where ProcessName != 'wmicprvse' | top
6
7 // Generated by Copilot
8 Process | where ProcessName != 'wmicprvse' | top
```

Get started **Results**

ProcessId	ProcessName	Path	CommandLine	Cur
88	Registry			
4	System			
0	System Idle Pro...			

Show the last 5 app crash events on this device

Ravi sees a number of processes associated with apps and wants to understand if the slowness might be caused by application crashes. He uses 'Query with Copilot' to ask for a query that can give him the last 5 app crash events on that device. He then runs this query to fetch this information.

Show the last 5 app crash events on this device

Here is a KQL query that can help you get that information.

KQL query

```
WindowsAppCrashEvent | order by LoggedDateTime desc | take 5
```

Add to editorAdd and run

How was this query generated?

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

▷ Run ✖ Clear input ✖ Cancel ↻ Query with Copilot

```
8 //Process | where ProcessName != 'wmiprvse' | top 5
9
10 // Generated by Copilot
11 WindowsAppCrashEvent | order by LoggedDateTime desc | take 5
```

Get started

Results

ReportId	AppPath	AppName	AppVersion	Log
5716	C:\Windows\...\\MoUs...\\MoUs...\\MoUs...	MoUsCoreWo...	1308.2407.1504...	202...
5579	C:\Windows\...\\MoUs...\\MoUs...\\MoUs...	MoUsCoreWo...	1308.2407.1504...	202...
5462	C:\Windows\...\\MoUs...\\MoUs...\\MoUs...	MoUsCoreWo...	1308.2407.1504...	202...

--	--

## Standalone SoC Scenarios

Jonas is a security expert that is investigating an incident. He needs to investigate a device that is potentially suspicious. This device is Intune managed and is currently in use. Jonas wants to know the differences in policies between this device and others, as well as potential known risks or threats.

Jonas begins his investigation by going to [Microsoft Copilot for Security](#) open prompt experience.

Prompt	Expected outcome
Show me the devices for the user u2544	Jonas asks Copilot for Security to show all the devices for the specified user. He verifies that Copilot provides him with information about the user and the devices associated with them.

	<p>Show me the devices for the user u2544</p> <p>&gt; <span style="color: green;">✓ 3 steps completed 15 seconds</span></p> <p>Oct 15, 1:13 PM</p> <h3>User Information</h3> <ul style="list-style-type: none"> <li><b>User ID:</b> e22d6804-aff5-4ed2-a2f1-0c1fa25ed17f</li> <li><b>Display Name:</b> u2544</li> <li><b>Usage Location:</b> FR</li> <li><b>User Principal Name:</b> <a href="#">u2544@ash.alpineskihouse.co</a></li> <li><b>Created Date:</b> 2024-09-17T22:48:17Z</li> </ul> <h3>User Groups</h3> <p>This user belongs to 12 user groups. For more details, visit <a href="#">User Groups</a>.</p> <h3>Devices</h3> <p>This user has a total of 2 Intune Managed devices.</p> <table border="1"> <thead> <tr> <th>Device Name</th><th>Intune Device ID</th><th>Enrolled Date</th></tr> </thead> <tbody> <tr> <td>FIELD-694635</td><td>7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc</td><td>2024-10-11T01:34:37+00:00</td></tr> <tr> <td>FIELD-340181</td><td>2feb9045-856a-4625-91a4-26cd56b08ab2</td><td>2024-10-11T01:31:34+00:00</td></tr> </tbody> </table> <p>To verify Intune managed devices in the Intune console, navigate to the <a href="#">Troubleshooting + support</a> page, choose Troubleshoot, and search using User Principal Name or Display Name: <a href="#">u2544@ash.alpineskihouse.co</a>.</p>	Device Name	Intune Device ID	Enrolled Date	FIELD-694635	7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc	2024-10-11T01:34:37+00:00	FIELD-340181	2feb9045-856a-4625-91a4-26cd56b08ab2	2024-10-11T01:31:34+00:00
Device Name	Intune Device ID	Enrolled Date								
FIELD-694635	7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc	2024-10-11T01:34:37+00:00								
FIELD-340181	2feb9045-856a-4625-91a4-26cd56b08ab2	2024-10-11T01:31:34+00:00								
Show me a summary of the device field-694635	He then asks about the potentially faulty device, and gets extensive information about its current configuration state.									

Show me a summary of the device field-694635

>  3 steps completed 19 seconds

Oct 15, 4:46 PM

## Summary of Device: FIELD-694635

The device **FIELD-694635** with ID **7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc** has the following policies:

### Device Configuration Policies

 Export to Excel



PolicyId	PolicyName	PolicyStatus
8bb111be-297d-444a-a69e-eb3e131f7a3d	Telemetry (for Autopilot devices)	Succeeded
7857d6a5-9b32-42e2-ad4a-2e80280009e8	Windows Health Monitoring (for Autopilot devices)	Succeeded
8bb111be-297d-444a-a69e-eb3e131f7a3d	Telemetry (for Autopilot devices)	Succeeded
7857d6a5-9b32-42e2-ad4a-2e80280009e8	Windows Health Monitoring (for Autopilot devices)	Succeeded

### Device Compliance Policies

 Export to Excel



PolicyId	PolicyName	PolicyStatus
c0f4911a-7ce6-4804-8563-677a2665d379	Default Device Compliance Policy	Compliant
22fc6a93-3336-4fc1-ab09-73abc2eb5092	Device Risk	Compliant

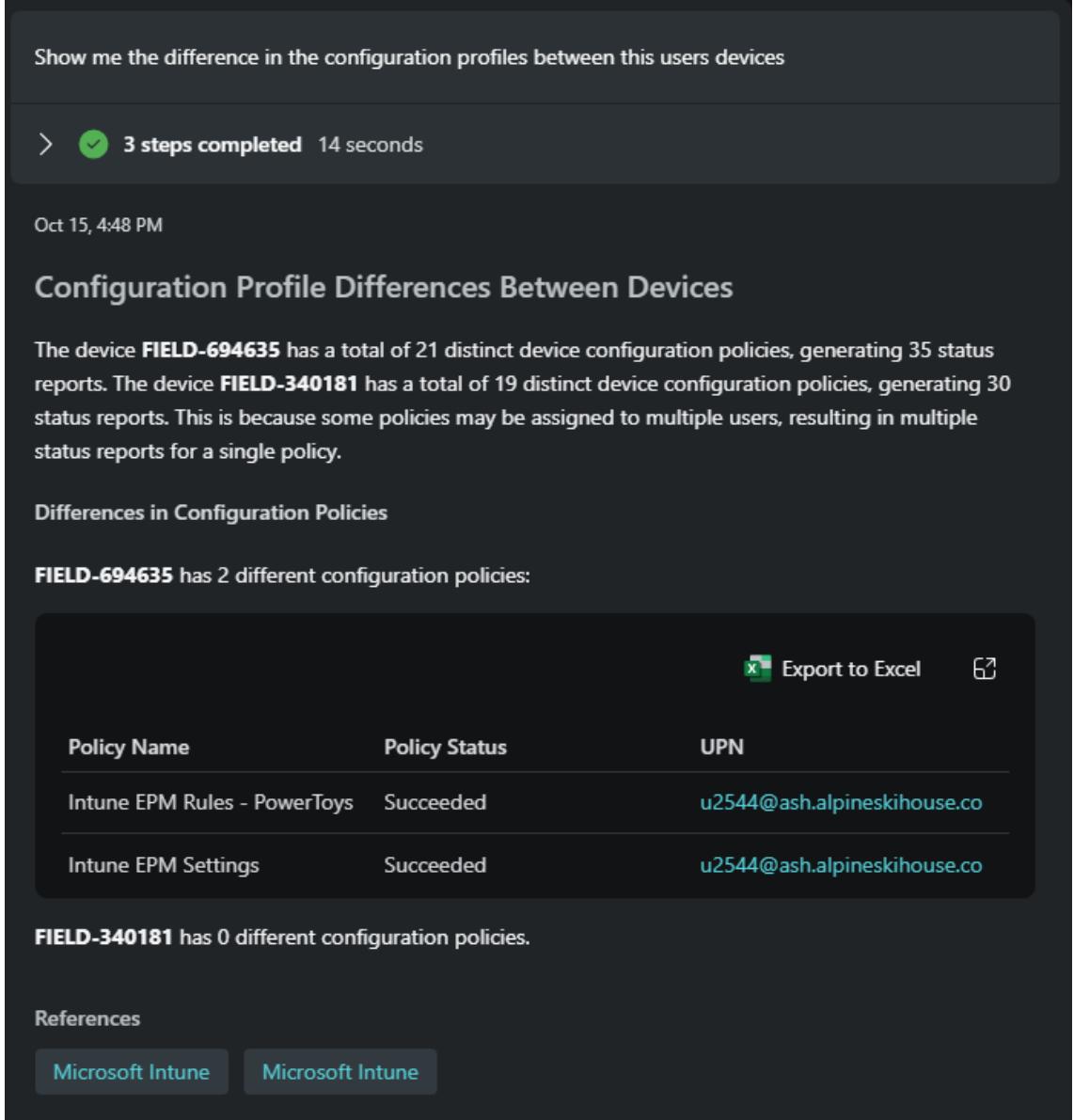
The device **FIELD-694635** has no application configuration policies.

### References

[Microsoft Intune](#)

[Microsoft Intune](#)

[Microsoft Intune](#)

<p>Show me the difference in the configuration profiles between this user's devices</p>	<p>He asks Copilot if there's any difference in configuration between the potentially compromised device and a known working and uncompromised device, so that he can determine if there is a missing setting causing an issue.</p>  <p>The screenshot shows a Copilot interface. At the top, a message says "Show me the difference in the configuration profiles between this user's devices". Below it, a progress bar indicates "3 steps completed" in 14 seconds. The date "Oct 15, 4:48 PM" is shown. The main content area is titled "Configuration Profile Differences Between Devices". It states that the device FIELD-694635 has 21 distinct policies and generating 35 status reports, while FIELD-340181 has 19 distinct policies and 30 status reports. It notes that some policies are assigned to multiple users. A section titled "Differences in Configuration Policies" lists two policies for FIELD-694635:</p> <table border="1" data-bbox="447 1056 1507 1347"> <thead> <tr> <th>Policy Name</th><th>Policy Status</th><th>UPN</th></tr> </thead> <tbody> <tr> <td>Intune EPM Rules - PowerToys</td><td>Succeeded</td><td>u2544@ash.alpineskihouse.co</td></tr> <tr> <td>Intune EPM Settings</td><td>Succeeded</td><td>u2544@ash.alpineskihouse.co</td></tr> </tbody> </table> <p>FIELD-340181 has 0 different configuration policies.</p> <p><b>References</b></p> <p><a href="#">Microsoft Intune</a> <a href="#">Microsoft Intune</a></p>	Policy Name	Policy Status	UPN	Intune EPM Rules - PowerToys	Succeeded	u2544@ash.alpineskihouse.co	Intune EPM Settings	Succeeded	u2544@ash.alpineskihouse.co
Policy Name	Policy Status	UPN								
Intune EPM Rules - PowerToys	Succeeded	u2544@ash.alpineskihouse.co								
Intune EPM Settings	Succeeded	u2544@ash.alpineskihouse.co								
<p>Show me the summary for the policy Intune EPM Rules – PowerToys</p>	<p>Jonas suspects the issue might be related to a specific policy – the Endpoint Privileged Protection policy – so he asks Copilot to summarize it, so he can quickly review it.</p>									

Show me the summary for the policy Intune EPM Rules – PowerToys

> **3 steps completed** 19 seconds

Oct 15, 4:49 PM

## Summary for Policy: Intune EPM Rules - PowerToys

### Policy Settings

- Elevation Rule Name - Applies to:** All device users
- Elevation Rule Name - File hash:**  
ECBEED67EFA864E558403F719B7FFD6F0192E77C36579B2FF9C2A0B6DD305752
  - Description:** Hash of the file that should be elevated
- Elevation Rule Name - Elevation type:** User confirmed
- Elevation type - Validation:** Unhandled setting type ChoiceCollection
- Elevation Rule Name - Child process behavior:** Allow all child processes to run elevated
- Elevation Rule Name - File name:** PowerToysSetup-0.68.1-x64.exe
- Elevation Rule Name - Rule name:** PowerToys

### Assignment Scope

- Included Groups:** Intune EPM Demo Devices
  - Member Count:** 1
  - Device Count:** 1
  - User Count:** 0

### Additional Information

- Elevation Rule Name:**
  - Benefits:** This setting allows administrators to create unique identifiers for specific rules, aiding in management and troubleshooting.
  - Adverse Impacts:** Mismanagement could lead to mistakes in rule application, potentially granting elevated privileges to incorrect applications or users.

### Summary

The policy "Intune EPM Rules - PowerToys" is configured to elevate the PowerToysSetup-0.68.1-x64.exe file for all device users, allowing all child processes to run elevated. The policy is assigned to the "Intune EPM Demo Devices" group, which includes one device. There are no conflicting policies found.

### References

[Microsoft Intune](#) [List of the settings in the Microsoft Edge s...](#)

Tell me about Intune setting "Child process behavior - Allow all child processes to run elevated"	<p>From the previous policy summary, Jonas suspects the issue might of originated from a specific setting, and that 'Child process behavior - Allow all child processes to run elevated', that might not be configured correctly.</p> <p>He asks Copilot to provide more information about this setting, so he can consider changing it.</p>
---------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Tell me about Intune setting "Child process behavior - Allow all child processes to run elevated"</p> <p>&gt;  3 steps completed 18 seconds</p> <p>Oct 15, 4:50 PM</p> <h3>Intune Setting: "Child process behavior - Allow all child processes to run elevated"</h3> <p>The Intune setting "Child process behavior - Allow all child processes to run elevated" is part of the Endpoint Privilege Management (EPM) policies. This setting allows any child processes created by an elevated process to also run with elevated permissions.</p> <p><b>Key Points:</b></p> <ul style="list-style-type: none"> <li>• <b>Default Setting:</b> By default, child processes require their own rule to be elevated.</li> <li>• <b>Allow All Child Processes:</b> This option allows all child processes to run elevated without requiring additional rules. It should be used with caution as it can potentially allow unapproved applications to gain elevated privileges [1].</li> <li>• <b>Deny All:</b> This configuration prevents any child process from being created.</li> </ul> <p><b>Important Considerations:</b></p> <ul style="list-style-type: none"> <li>• <b>Security Implications:</b> Allowing all child processes to run elevated can pose security risks if not managed properly. It is crucial to ensure that only trusted applications are allowed to use this setting [1].</li> <li>• <b>Compatibility Issues:</b> Changing the child process behavior may cause compatibility issues with certain applications that expect the default Windows behavior. Thorough testing is recommended when manipulating this setting [2].</li> </ul> <p>For more detailed guidance on creating strong rules and managing child process behavior, refer to the guidance for creating elevation rules with Endpoint Privilege Management [1].</p> <p><b>References</b></p> <p><a href="#">Windows elevation rules policy</a>   <a href="#">Important concepts for Endpoint Privilege ...</a></p>
What are the threats	Lastly, Jonas asks Copilot if there are any threats associated with this user's devices, to ensure the environment remains safe.

associated  
with this  
users  
devices?

What are the threats associated with this users devices?

> 3 steps completed 26 seconds

Oct 15, 4:52 PM

## Threats Associated with User's Devices

The following KQL query was used to identify threats associated with the devices for the user u2544:

```
1 let userDevices = IntuneDevices
2 | where UserName == "u2544"
3 | project DeviceId;
4
5 AlertEvidence
6 | where DeviceId in (userDevices)
7 | join kind=inner (AlertInfo) on AlertId
8 | project Timestamp, AlertId, Title, Category, DeviceId, DeviceName,
ThreatFamily, Application, ApplicationId
```

**Product Name:** Defender

**Total Row Count:** 0

**Displayed Row Count:** 0

**KQL Output Result Data:** No Data

No data found in the table. Check if the requested data is streaming into the relevant Microsoft product correctly.

**References**

[Go hunt in Microsoft 365 Defender](#)

[Sample session](#) from Alpine Ski House.

## Activity 5: Purview Use Cases

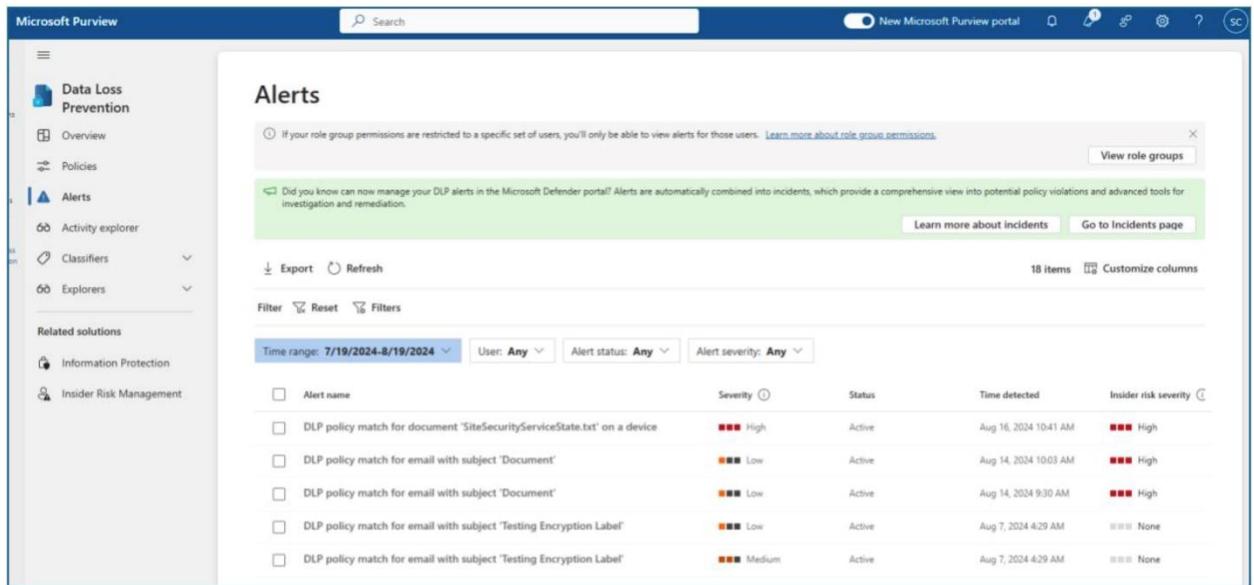
### Estimated time to complete this activity

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.



The screenshot shows the Microsoft Purview Data Loss Prevention Alerts interface. The left sidebar has a 'Data Loss Prevention' section with 'Overview', 'Policies', and 'Alerts' selected. Under 'Alerts', there are 'Activity explorer', 'Classifiers', and 'Explorers'. Below that are 'Related solutions' for 'Information Protection' and 'Insider Risk Management'. The main area is titled 'Alerts' and displays a list of alerts. A message bar at the top says, 'Did you know you can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically combined into incidents, which provide a comprehensive view into potential policy violations and advanced tools for investigation and remediation.' Below the message are 'Learn more about incidents' and 'Go to Incidents page' buttons. There are 'Export' and 'Refresh' buttons, and filters for 'Time range: 7/19/2024-8/19/2024', 'User: Any', 'Alert status: Any', and 'Alert severity: Any'. The alert list table has columns for 'Alert name', 'Severity', 'Status', 'Time detected', and 'Insider risk severity'. The table lists several alerts, all of which are 'Active' and have a 'High' severity level. The first alert is 'DLP policy match for document 'SiteSecurityServiceState.txt' on a device'.

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**

- N 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**

- N 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



### 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 d1146bf2fa-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. 

Copy to clipboard  
 Regenerate  
 Open in Copilot for Security

## 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 has columns for ID, Copilot, Users, Policy, Status, Spotlight, Alert severity, Time detected, Assigned to, Case, and Case status. The first few rows show alerts for users like Lee Gu, Ismat Belarevich, Lisa Monville, Nima Melany, Debra Berger, and Account Admin.

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

This screenshot shows the same Microsoft Purview Alerts page but with a search filter applied. The search bar at the top right contains the text "isaiah". Below the search bar, it says "1 of 9 selected". The main table now only displays alerts related to the user "Isaiah Langer". The rows listed are:

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

The screenshot shows the Microsoft Copilot interface, which has integrated the alert summary. The summary is titled 'Alert summary' and includes the date 'Aug 19, 2024 1:51 PM'. It provides a detailed breakdown of the alert, mentioning the user 'isaiah@woodgrove.ms' and the triggering event 'HR connector imported a resignation date'. The summary also lists several key findings and context, such as the user being a member of a priority user group and the detection of sensitive SharePoint file access. A red box highlights the 'Copilot' icon in the top right corner.

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**

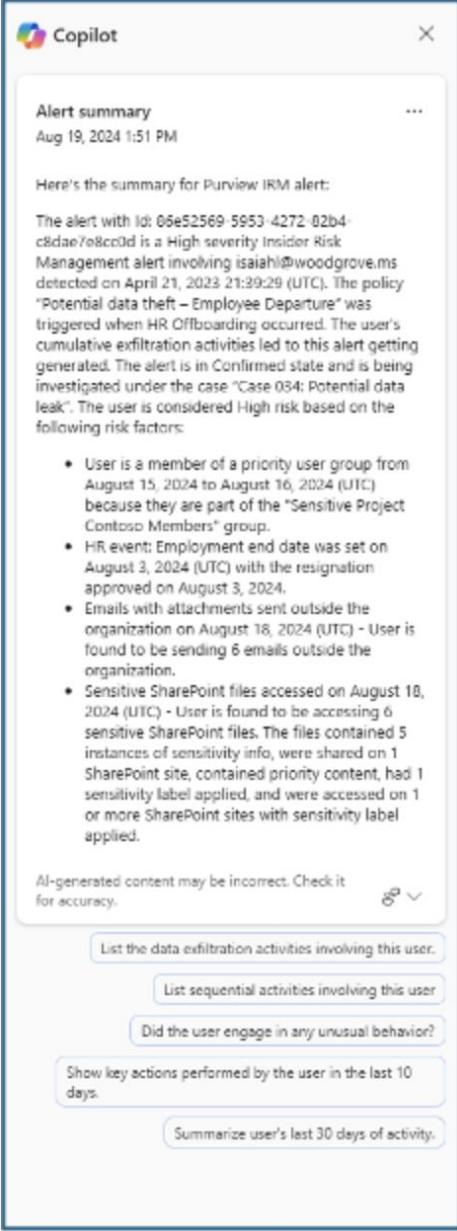
(1) Priority user groups are not currently supported for use with Admin Units. It is recommended to ensure that the reviewers of a priority user group are not restricted to specific admin units. [Learn more about admin units.](#) [X](#)

The screenshot shows the Microsoft 365 Copilot Alerts interface. At the top, there's a header with a 'Spotlight' icon, a search bar containing 'isaiah', and a 'Customize columns' button. Below the header is a toolbar with 'Summarize with Copilot', 'Export', 'Dismiss alerts', and 'Assign' buttons. A message box at the top left says: '(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.](#)'

The main area is a table listing alerts. The columns are: ID, Copilot, Users, Policy, Status, Spotlight, Alert severity, Time detected, Assigned to, Case, and Case status. There are 9 selected alerts. One alert for user 'isaiah' is highlighted with a red box around the Copilot column.

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

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

A screenshot of a Microsoft Copilot alert summary window. The window title is "Copilot" and the main section title is "Alert summary". The date is Aug 19, 2024 1:51 PM. The content area starts with a summary of a Purview IRM alert, mentioning an ID, a user email, and a detection date. It then lists several risk factors, each preceded by a bullet point. At the bottom left, there's a note about AI-generated content being incorrect and a checkmark icon. Below the main content are five rectangular buttons with text: "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.", and "Summarize user's last 30 days of activity.".

Alert summary

Aug 19, 2024 1:51 PM

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. 

List the data exfiltration activities involving this user.

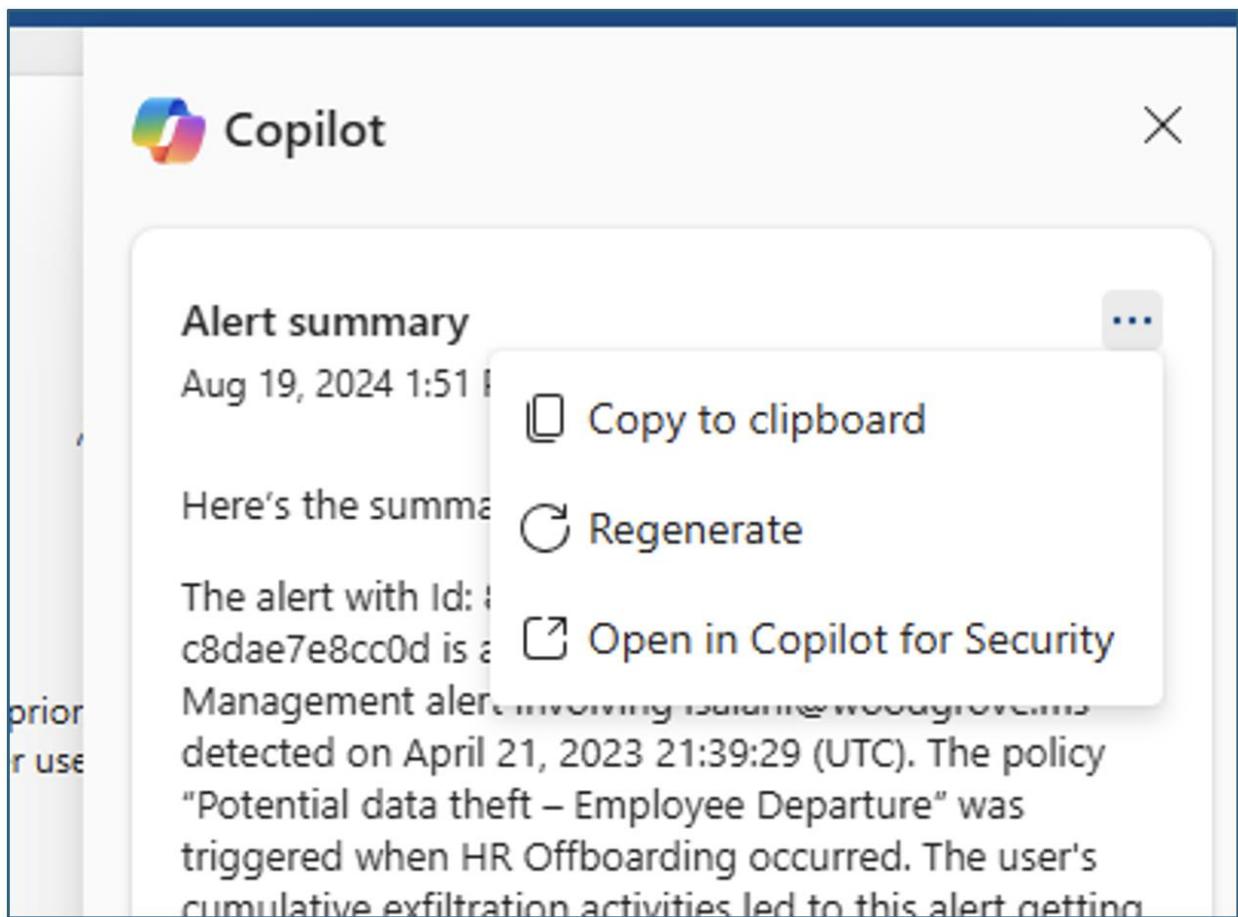
List sequential activities involving this user.

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 isaiahl@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 isaiahl@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.

I (Risk s  
ed to  
449  
4  
riority cor  
814 act  
ntent  
ew all pr

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

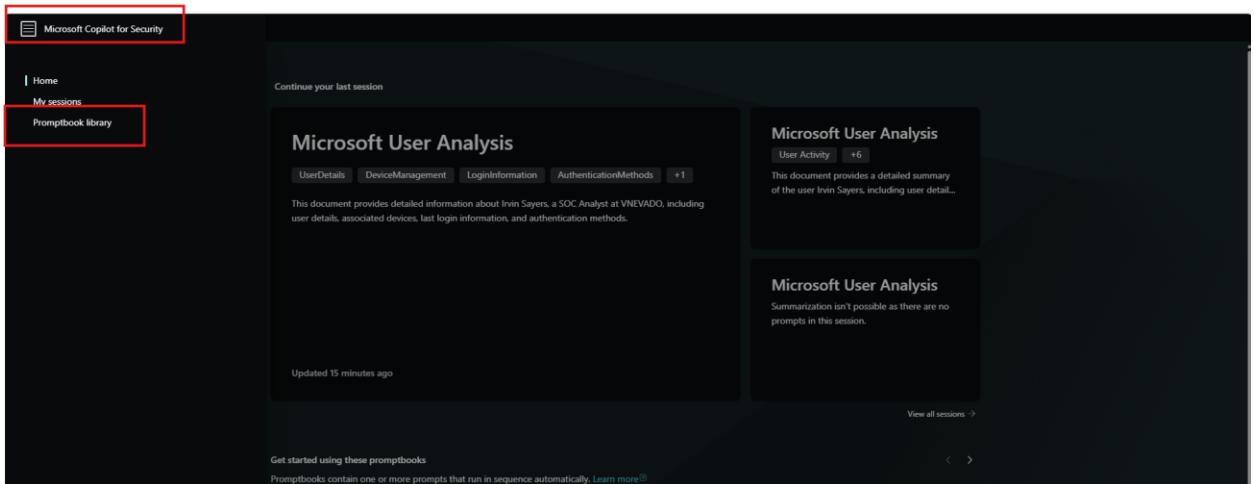
Estimated time to complete this activity

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



The screenshot shows the Microsoft Copilot for Security interface. On the left, there is a navigation bar with three items: 'Home' (disabled), 'My sessions' (disabled), and 'Promptbook library'. The 'Promptbook library' item is highlighted with a red box. In the center, there is a 'Microsoft User Analysis' card for a user named Irvin Sayers. The card includes tabs for 'UserDetails', 'DeviceManagement', 'LoginInformation', and 'AuthenticationMethods'. It also shows '+1' new items. Below the card, it says 'This document provides detailed information about Irvin Sayers, a SOC Analyst at VNEVADO, including user details, associated devices, last login information, and authentication methods.' At the bottom of the card, it says 'Updated 15 minutes ago'. At the very bottom of the page, there is a note: 'Get started using these promptbooks' and 'Promptbooks contain one or more prompts that run in sequence automatically. [Learn more](#)'.

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

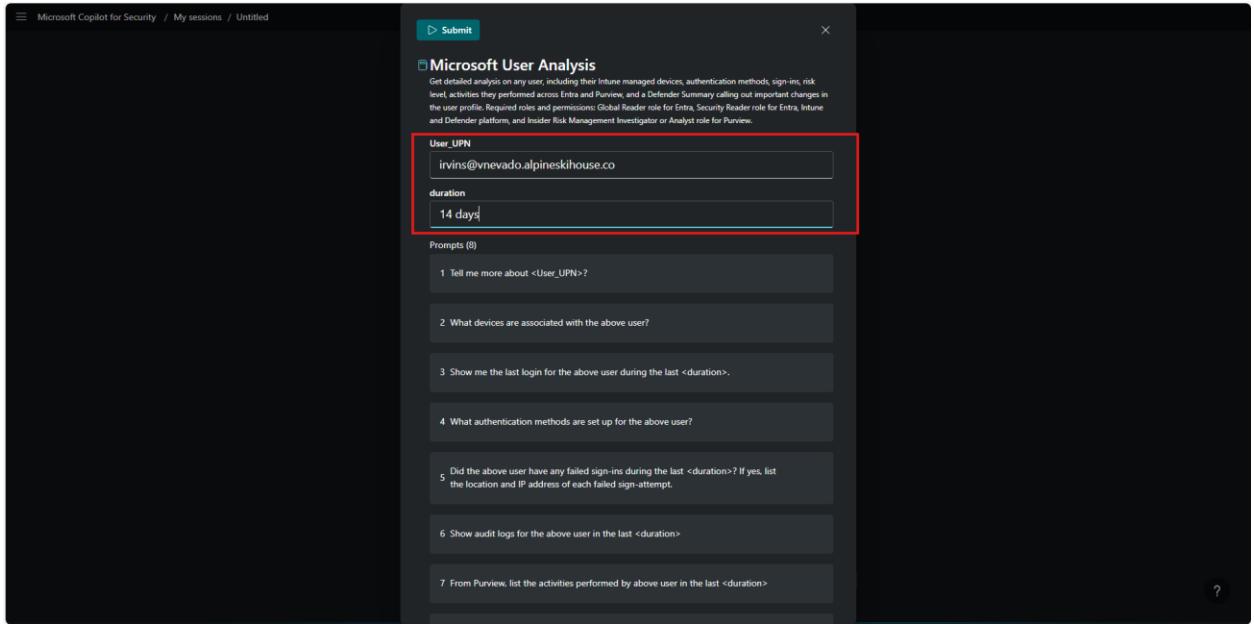
The screenshot shows the Microsoft Copilot for Security interface with the "Promptbook library" tab selected. A search bar at the top has "Microsoft" typed into it. Below the search bar, there is a filter section with dropdowns for "All", "My promptbooks", and "Alpine Ski House". The main area displays a list of promptbooks. One promptbook, "Microsoft User Analysis", is highlighted with a red box. This promptbook 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: Global Reader role for Entra, Security Reader role for Entra, Intune and Defender platform, and Insider Risk Management Investigator or Analyst role for Purview." It has 8 prompts and is owned by Microsoft.

5. Click on “Start a new Session”

The screenshot shows the Microsoft Copilot for Security interface with the "Promptbook library" tab selected. The "Microsoft User Analysis" promptbook is open in a modal window. At the top of this window is a blue button labeled "Start new session". The main content area of the modal shows the details of the promptbook, including its description and required roles. Below this, under the heading "Inputs you'll need", there is a field for "User\_UPN" with "duration" specified. Under the heading "Prompts", there is a numbered list of 7 questions:

- 1 Tell me more about <User\_UPN>?
- 2 What devices are associated with the above user?
- 3 Show me the last login for the above user during the last <duration>.
- 4 What authentication methods are set up for the above user?
- 5 Did the above user have any failed sign-ins during the last <duration>? If yes, list the location and IP address of each failed sign attempt.
- 6 Show audit logs for the above user in the last <duration>.
- 7 From Purview, list the activities performed by above user in the last <duration>

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



## 7. Go through the results

## 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. On the left, there's a navigation pane with sections like Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, and Show more. A red box highlights the 'Protection' section, which contains Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, and Risky activities. Another red box highlights the 'Risky activities' link under the Protection section. The main area is titled 'Security | Risky users' and displays a table of risky users. The table has columns for User (with a dropdown arrow), Risk state (At risk), and Last updated. The table lists several users, including Lee Gu, with their respective details.

User	Risk state	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.