

Security Copilot Flight Simulator – Hands on Workshop Lab Guide Americas 2025



!! Disclaimer: All exercises in this lab are based on the current environment at Alpine Ski House and are subject to change. Incidents, alerts, user status, and risk levels can vary over time, which may result in different responses. While we strive to keep the materials updated, we cannot guarantee their accuracy at all times.

Table of Contents

Agenda.....	3
Activity 1: Let's Get Familiar with Security Copilot	4
Exercise 1: Security Copilot Standalone Experience.....	4
Explore Security Copilot Standalone Experience	4
Activity 2: Microsoft Defender XDR	8
Exercise 1: Incident Summary and Guided Response	9
Exercise 2: Incident Report	12
Exercise 3: Entity deep dive investigation - Script Analyzer	15
Exercise 4: Entity deep dive investigation - File Analyzer.....	16
Exercise 5: Entity deep dive investigation - Device Summary	18
Exercise 6: Natural Language Query Assistant in Advanced Hunting	19
Exercise 7: Defender XDR Standalone	21
Activity 3: Microsoft Entra	22
Exercise 1: Risky users summarization.....	22
Exercise 2: Risky App Investigation	23
Exercise 3: Entra Standalone	25
Activity 4: Microsoft Purview	26
Exercise 1: Microsoft Purview Data Loss Prevention.....	27
Exercise 2: Microsoft Purview Insider Risk Management	31
Exercise 4: Microsoft Purview Communication Compliance.....	35
Exercise 4: Microsoft Purview eDiscovery	39
Exercise 5: Microsoft Purview Data Security Posture Management (DSPM).....	44
Exercise 6: Microsoft Purview DLP Policy Insights with Copilot.....	46
Exercise 7: Microsoft Purview Standalone.....	48
Activity 5: Intune	54

Exercise 1: Policy Management – Setting Information, Conflicts and User and Security Impact Assessment	54
Exercise 2: Policy Management: Summarization and Security Impact Assessment	61
Exercise 3: Troubleshooting – Device summarization and Comparison.....	66
Exercise 4: Troubleshooting – Error Codes	70
Exercise 5: Copilot into Single Device Query	73
Exercise 6: Intune Standalone	78
Activity 6: Standalone and Extensibility.....	84
Exercise 1: Running built-in Promptbook	84
Exercise 2: Create a Promptbook	87
Exercise 3: Custom Plugin (Walkthrough only)	88

Agenda

TIME	EVENT	DETAILS
9:00–9:30 AM	Breakfast	Check In and Breakfast
9:30–10:00 AM	Welcome	Security Copilot Overview
10:00–12:00 PM	Workshop basics, workflows, and use cases	Lab setup and introduction (15 Mins) - Explore standalone experience - User/role management, auditing - Manage plugins & skills Security Copilot Embedded + Standalone (2 hours) - Copilot in Microsoft Defender XDR - Copilot in Microsoft Entra - Copilot in Microsoft Purview - Copilot in Microsoft Intune
12:00–1:00 PM	Lunch & small group discussions	Break and over lunch discuss workflows can be used within your organization
1:00-2:30	Workshop promptbook take-home	Standalone & Extensibility (30 Mins) - Built-in Promptbooks & Custom Plugin Promptbook Engineering (1 hour)
2:30-3:00	Q&A	Q&A and Feedback

Activity 1: Let's Get Familiar with Security Copilot

Estimated time to complete this activity

15 minutes

Exercise 1: Security Copilot Standalone Experience

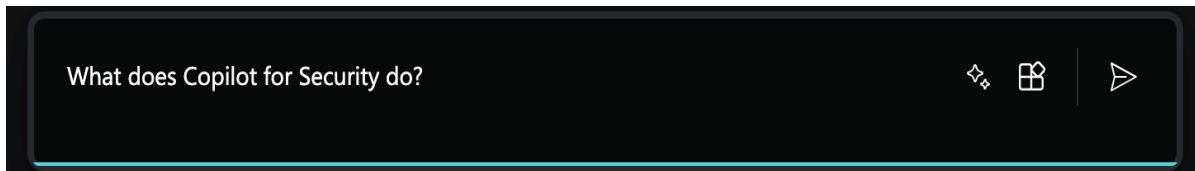
In this exercise, you will explore the Security Copilot Standalone Experience. You will learn how to navigate the portal, manage plugins, and utilize various features to enhance your security operations. This hands-on activity will help you become familiar with the capabilities of Security Copilot and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

Explore Security Copilot Standalone Experience

1. Open your browser, and go to the Copilot for <https://securitycopilot.microsoft.com/> (Login with your Alpine Ski house account)
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.
Following requires Security Copilot Owner role
 - d. **Owner settings** includes capacity management, data sharing feedback and options, plugin management, logging audit management and manage data access from Microsoft 365 services
 - e. **Role assignment** user access management, control who has access to Security Copilot by adding or removing users, groups, Entra ID roles, or managed identities
 - f. **Usage monitoring** view/monitor security compute units use

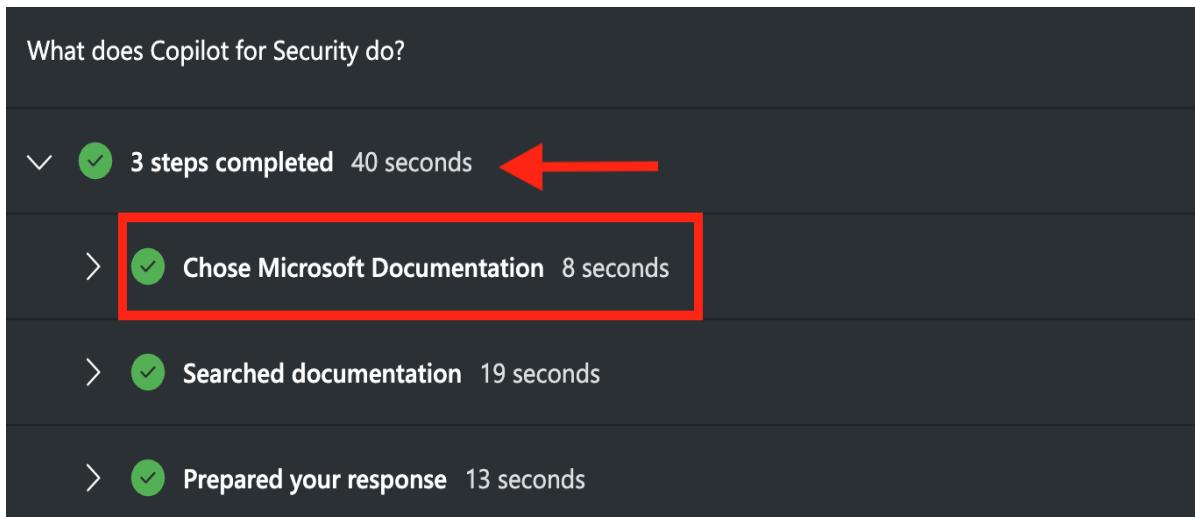
⚠️ Important Remark: Since your account has the Contributor role in Alpine Ski House, not all options are visible. Owners can manage capacity, data evaluation, see usage and more.

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 Security Copilot do?**



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

 **Tip:** Notice the plugin selected was ‘Microsoft Documentation’ by the Security Copilot Orchestrator. Microsoft Copilot orchestrator works behind the scenes to select and execute the right plugin and skill(s).



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 Security Copilot 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 Security Copilot 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.

The screenshot shows the 'SYSTEM CAPABILITIES' section. It includes a red arrow pointing from the 'See all system capabilities' link to the 'See all system capabilities' link in the main text below. The section lists three capabilities:

- 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 thread intelligence plugin.
10. Let's select "**Get CVE by ID**" and review the input that this skill required.

The screenshot shows the 'Get CVE details by IDs' skill interface. It has two input fields: 'CVE-2024-3400' and 'Summary'. A large blue 'Run' button is at the bottom right.

11. In the input parameter add the, **CVE-2024-3400** and **Summary** 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.

Security Copilot 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 his 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:** Security Copilot 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 three filter buttons ('All (29)', 'On (10)', 'Off (19)') are at the top. Below is a list of Microsoft services as plugins:

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

Activity 2: Microsoft Defender XDR

The objective of this activity is to familiarize participants with Security Copilot embedded features and demonstrate the value they bring in Defender XDR portal. 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.

This exercise involves investigating a Human-Operated Ransomware attack using Microsoft Defender XDR and Security Copilot. 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.

Estimated time to complete this activity

35 minutes

Exercise 1: Incident Summary and Guided Response

1. Navigate to Defender XDR portal (<https://security.microsoft.com>) and login with your Alpine Ski House credentials
2. Go to **Investigation & response > Incidents & alerts > Incidents**
3. In the incident search bar, enter "**Human-operated ransomware attack**" and hit enter

The screenshot shows the Microsoft Defender XDR portal's incident search interface. A red arrow points to the search bar which contains the query "human-operated ra...". Below the search bar are various filters: Status: Any, Alert severity: Any, Incident severity: Any, Incident assignment: Any, Incident name, Incident Id, Tags, Severity, and Investigation. The search results list one incident: "Human-operated ransomware attack was launche... 107". This incident is categorized under "Ransomware" with 8 sub-items, has a "High" severity level, and is associated with 3 investigations.

4. Open the **Incident Id 4078** (Direct url: <https://security.microsoft.com/incident2/4078>) or the most recent incident by clicking on it > Upon opening the incident, Copilot automatically summarizes the incident into **Incident Summary** with most valuable information to help you quickly assess the incident status and risk to take the first action immediately.

 **Tip:** Review the generated summary and involved files. This is a great example of ROI to business

5. The Copilot pane appears on the right side also shows the **Guided Response cards**.

<p>Review the Triage response cards.</p> <p>1. Triage is a critical step in the Security CoPilot guided investigation process. It involves the initial assessment and prioritization of security alerts and incidents to identify and dismiss false positives to avoid unnecessary investigations. This helps in focusing resources on genuine threats.</p>	<p>The screenshot shows the Triage pane with the following content:<ul style="list-style-type: none">A blue circular icon with a white dot labeled "New".The text "Confirm this is a 'true positive'".The date and time "Aug 22, 2024 1:55 PM".The text "Your organization has classified similar incidents as a 'true positive'."A "Classify" button with a dropdown arrow.A green-bordered "View similar incidents" button.A note at the bottom: "AI-generated content may be incorrect. Check it for accuracy." with a "Check" button.</p>
---	---

2. Select **Similar incidents** to navigate to another incident in Microsoft Defender XDR, the logic typically involves examining various aspects such as entities involved, timelines, and patterns.

Entities -Users, Devices, Files, Processes

Timeline - Initial Compromise, Lateral Movement, Exfiltration, Mitigation Actions

Patterns and Correlations - Common Attack Vectors, Repeated IoCs, Behavioral Patterns

In the triage card, Copilot recommends actions for triage if it is available. And if available, you can also view similar incidents to assist you in triaging the new incident and see the actions previously taken to speed up your triage and investigation. If confident, Copilot provides a clear verdict suggestion

Note: This is a shared environment. Please avoid making any changes or updates.

	Triage	Not set
	● New	True positive
	Confirm this is a Aug 22, 2024 1:55 P	Multi staged attack
	Your organization	Malware
	as a 'true positive'	Malicious user activity
	Classify ▾	Unwanted software
	AI-generated conte it for accuracy.	Phishing
		Compromised account
	Containment	Other
	● New	Informational, expected activity
	Isolate device av win1h.avoriaza	Security testing
	Aug 22, 2024 1:55 P	Confirmed activity
	Other organizatio	Line of business application
	similar incidents.	Other
	Isolate device	False positive
	AI-generated conte it for accuracy.	Not malicious
	● New	Not enough data to validate
	Isolate device av dc.avoriaz.alpine	Other

<p> This containment response card respects user permissions. If the user lacks the necessary permissions, the action will be disabled.</p> <p>Review the different Containment response cards (if available)</p>	<p>Completed</p> <p>Disable the account Lynne Robbins</p> <p>Sep 24, 2024 12:09 AM</p> <p>Attack Disruption</p> <p>AI-generated content may be incorrect. Check it for accuracy.  </p>
<p>Copilot provides containment actions like “isolate device” or “disable user” to stop attacks immediately. You also get information about automated actions that contained the incident like attack disruption</p>	<p>Completed</p> <p>Contain device</p> <p>Sep 24, 2024 12:09 AM</p> <p>Attack Disruption</p> <p>AI-generated content may be incorrect. Check it for accuracy.  </p>
<p>Review the different Investigation response cards. Select a response card and show the investigation response action that Copilot suggested</p>	<p>Copilot generates a predefined text you can “Copy to Clipboard” to use to start communication with an affected user to confirm their activity</p>
<p>Scroll down to the Remediation cards in guided response</p>	<p>Copilot recommends remediation actions like “force password reset,” “revoke user session,” and “disable inbox rule” to prevent attacks from further spreading</p>

 **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.

Exercise 2: Incident Report

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

Select the **report icon** found on top of the Copilot side panel to generate the incident report.

Copilot

Incident summary

Aug 22, 2024 3:35 PM

The high severity incident 'User account compromise identified from a known attack pattern' occurred between 2024-04-25 09:59:34 UTC and 2024-04-30 19:36:44 UTC. It was tagged as Credential Phish and Ransomware, and triggered an automatic Attack Disruption action.

- **Collection:** The incident began at 2024-04-25 09:59:34 UTC when a suspicious inbox forwarding rule was set on the inbox of user 'sonia', indicating a possible account compromise. The rule forwards all incoming

[See more](#)

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

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

Copilot

Manage incident

...

Run playbook

Activity log

Ask Defender Experts

Generate incident report

Export incident as PDF

Summary
3:35 PM

User account compromise identified from a known attack pattern occurred between 2024-04-25 09:59:34 UTC and 2024-04-30 19:36:44 UTC. It was tagged as Credential Phish and Ransomware, and triggered an automatic Attack Disruption action.

The incident began at 2024-04-25 09:59:34 UTC when a suspicious inbox forwarding rule was set on the inbox of user 'sonia', indicating a possible account compromise. The rule forwards all incoming

[See more](#)

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

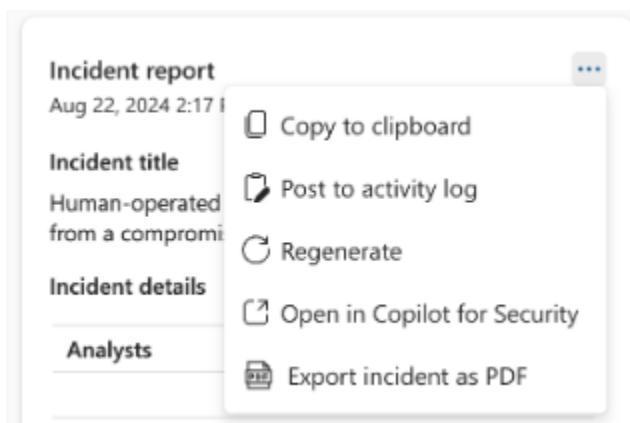
Post-incident, security teams need to document the event and their response. Copilot simplifies incident reporting by generating comprehensive and contextualized activity reports that combine incident response data like analysts' activities and actions within an incident.

Incident report	...
Aug 22, 2024 5:04 PM	
Incident title	User account compromise identified from a known attack pattern (attack disruption)
Incident details	
Analysts	Mimik Emails - AlpineSkiHouse adm_ajourn@seccxpdemo.on... Defender Experts jafafner@microsoft.com rafikmezil@microsoft.com tiandert@microsoft.com yishayperry@microsoft.com chutchings@microsoft.com Filiz.Babacan@microsoft.com msalih_microsoft.com#EXT#...
Time created	04/25/2024 09:59:34
First log	04/25/2024 10:10:27
Last log	08/18/2024 13:15:37
Time closed	-
Incident summary	The high severity incident 'User account compromise identified from a known attack pattern' occurred between 2024-04-25 09:59:34 UTC and 2024-04-30 19:36:44 UTC. It was tagged as Credential Phish and Ransomware and triggered an automatic Attack Disruption action.
	<ul style="list-style-type: none">Collection: The incident began at 2024-04-25 09:59:34 UTC when a suspicious inbox forwarding rule was set on the inbox of user 'sonia'. This rule forwarded all incoming email to the external address it@contosodonotexists.com, indicating a possible compromise and information

Copilot converts different response activities taken from these sources like analyst case comments, manual and automated

	activities and summarizes them into one report. Copilot incident report can also perform advanced steps like estimating which manual actions were connected to the incident response flow
--	---

2. Once generated, the report can be a) **Copy to clipboard** to copy to your preferred system, b) **Post to activity log** within the Incident for record-keeping and refer to actions of an incident for future decision-making, and c) **Export incident as PDF** for reporting purposes.



Exercise 3: Entity deep dive investigation - Script Analyzer

Copilot's script analysis capability allows security teams to easily review scripts and command lines in all languages, including encoded ones. It translates scripts into natural language, highlighting and explaining key parts, enhancing team skills and reducing investigation time.

1. Within the Incident Id [4078](#), in the attack story, select the alert “Suspicious PowerShell command line” and expand the **[7660] powershell.exe - EncodedCommand**. Click **Analyze** on the encoded script. The script analysis results will show on the Copilot side panel.

The screenshot shows the Microsoft Defender XDR interface for an incident titled "Human-operated ransomware attack was launched from a compromised asset (attack disruption)". The timeline on the left lists several events:

- Jan 17, 2025 5:20 AM: Resolved Mimikatz credential theft tool (vnevado-win10vnevado.alpineskihouse.co)
- Jan 17, 2025 5:20 AM: Resolved Mimikatz credential theft tool (vnevado-win10vnevado.alpineskihouse.co)
- Jan 17, 2025 5:20 AM: Resolved Suspicious PowerShell command line (vnevado-win10vnevado.alpineskihouse.co)
- Jan 17, 2025 5:20 AM: Resolved Suspicious access to LSASS service (vnevado-win10vnevado.alpineskihouse.co)
- Jan 17, 2025 5:20 AM: Resolved PsExec launched a command on a

The "Suspicious PowerShell command line" event is highlighted with a red box. To its right, a detailed view of the PowerShell command is shown:

```

powershell.exe executed a script
Content
Analyze
curl www.voyagorclub.space
function Get-UserPRToken
Content SHA256
b134e88760506ea2e1c385dc0987637f055586eac1a
38e19e2aaca8d51d7678

```

The "Analyze" button is also highlighted with a red box.

2. Select **Show code** to expand the script and describe the script analysis results. To close the expanded results, select **Hide code**

Exercise 4: Entity deep dive investigation - File Analyzer

File analysis capability, like script analysis, extends analysts' capacity to examine files instantly. Analysts can quickly triage a file based on the overview and can conduct deeper investigation into a file with the detailed analysis provided

3. Within the same Incident, click on **File** icon from the **Incident graph** attack story > **View Files**

The screenshot shows the Microsoft Defender XDR interface. On the left, under 'Attack story', there is a list of four alerts:

- Aug 29, 2024 10:53 PM Resolved Potential human-operated malicious activity vnevado-win10vnevado.alpineskihouse.co
- Aug 30, 2024 3:08 AM Resolved Suspicious RDP session vnevado-win10vnevado.alpineskihouse.co jonaw
- Aug 30, 2024 3:10 AM Resolved Suspected overpass-the-hash attack (Kerberos) VNEVADO-Win10vnevado.alpineskihouse.co Lynne Robbins
- Aug 30, 2024 3:10 AM Resolved Suspicious PowerShell command line vnevado-win10vnevado.alpineskihouse.co jonaw

On the right, the 'Incident graph' shows a network of nodes representing various entities like hosts, users, and files. A tooltip for a file node indicates 'View 11 Files'. There are also buttons to 'Pin related alerts', 'Hide related alerts', and a legend for 'Communication' and 'Association'.

4. Select the file **Mimikatz.exe** file from the list. > select the file to analyze from the list (**mimikatz.exe**) > click **Analyze**. Copilot will automatically provide a file analysis summary in the file page

The image contains two side-by-side screenshots of the Microsoft Defender XDR file analysis interface.

Left Screenshot: Shows a list of 11 files associated with the alert. The files listed are: Orchestrator.ps1, mimidrv.sys, mimidrv.sys, mimikatz.exe, mimilib.dll, mimispool.dll, mimikatz.exe, mimilib.dll, and mimispool.dll.

Right Screenshot: Shows the details for the mimikatz.exe file. It includes a preview icon, a 'File' button, and a prominent red box around the 'Analyze' button. Below the file name, it displays 'Detection' information: 'VirusTotal detection ratio' (63/70) and 'Malware detected' (Multiple mal...).

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.

Exercise 5: Entity deep dive investigation - Device Summary

To determine the extent of an attack, it's crucial to understand how a specific device is connected to the incident and what other components might be compromised.

Security Copilot can generate a device summary instantly, providing a comprehensive view of the device's security state without the need to sift through vast amounts of data.

1. Within the same incident page, click on **Devices** icon from the **Incident graph** attack story > **View Devices** or navigate to **Assets > Devices**
2. Click on device **vnevado-win10v.vnevado.alpineskihouse.co**

Device Name	Domain
vnevado-jump.vnevado.alpineskihouse.co	vnevado.alpineskihouse.co
vnevado-win11t.vnevado.alpineskihouse.co	vnevado.alpineskihouse.co
vnevado-win11u.vnevado.alpineskihouse.co	vnevado.alpineskihouse.co
vnevado-win10v.vnevado.alpineskihouse.co	vnevado.alpineskihouse.co

3. Click on Summarize to generate an analysis of this device

The screenshot shows a device summary page for a Windows 10 virtual machine named 'vnevado-win10v'. At the top, there's a blue circular icon with a white laptop symbol. Below it, the device name 'vnevado-win10v' is displayed. A legend indicates 'Medium' with a yellow square and 'Criticality: Very high' with a yellow square followed by four smaller ones. Below the device name, two tabs are visible: 'AlpineSkiHouse' (selected) and 'ModernWork - Semi automation'. A red box highlights the 'Summarize' button, which has a blue icon of a document with a magnifying glass. Other buttons include 'Open device page' (with a plus sign), 'View in map' (with a location pin), and a three-dot menu. The main content area is titled 'Hardware and firmware' and contains sections for 'System model' (No information available), 'Processor model' (Intel Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz), 'BIOS' (No information available), and a 'See all details' link.

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

Exercise 6: Natural Language Query Assistant in Advanced Hunting

Copilot plays a crucial role in supporting novice threat hunters who are still learning the Kusto Query Language (KQL) and the advanced hunting data schema. By providing guided assistance and query suggestions, Copilot helps hunters quickly craft KQL queries, get up to speed, enhancing their skills and confidence in threat hunting.

1. From the existing Incident view, click on any entity > **Actions** > **Go Hunt** (or within the Defender XDR portal, navigate to **Investigation & response** > **Hunting** > **Advanced hunting**). Click on Copilot icon to open load/access Copilot prompt

⚠️ Important Remark: The maximum lookback time is 30 days for XDR tables, while Sentinel lookback time depends on the retention period configured for tables. However, note that KQL can refer to any time range so there will be no error if you specify a longer lookback time. For demo purposes, we suggest using a lookback time according to the maximum.

2. Within the advanced hunting, Copilot provides query suggestions to help you frame your questions effectively, enabling you to go beyond incident investigation and engage in proactive threat hunting
3. In the prompt bar on the Copilot side panel, ask Copilot to **list all of Lee Gu sign ins in the last 30 days**. You can tweak the number of days based on an incident's details.

- Click Run Query under the returned KQL to run the query (if the query doesn't run, copy and paste the KQL in the query window and run to view the results)
4. Ask an additional question to generate a new/different query and show how Copilot stays in context

- a. For example, ask Copilot to ***list all his sign ins from non-US locations in the last 30 days***

Click Run Query under the returned KQL to run the query (if the query doesn't run, copy and paste the KQL in the query window and run to view the results)

Exercise 7: Defender XDR Standalone

In this exercise, you will investigate the same incident (Incident Id 4078) using Security Copilot standalone

1. Login to Security Copilot [<https://securitycopilot.microsoft.com>] and start a new session
2. In the prompt bar enter **Give me a summary of Defender incident 4078.**
3. Ask the Security Copilot the following example questions to gain deeper insights and ensure a thorough understanding of the incident
 - a **Incident Details:**
 - o What was the start time and date of the incident?
 - o Which entity or asset was initially compromised?
 - o Can you provide a timeline of how the attack unfolded?
 - b **Impact Assessment:**
 - o What assets were affected by the incident?
 - o Were there any critical systems or data impacted?
 - o What is the estimated scope and impact of the attack?
 - c **Indicators of Compromise (IoCs):**
 - o What IoCs were identified during the incident?
 - o Are there any known threat actors associated with these IoCs?
 - d **Response Actions:**
 - o What actions were taken to mitigate the incident?
 - o Were there any automated responses triggered?
 - o What manual steps did analysts take during the incident response?
 - e **Threat Intelligence:**
 - o Is there any additional threat intelligence related to this incident?
 - o Can you summarize the latest threat activity involving similar attacks?
 - f **Recommendations:**
 - o What are the recommended next steps to prevent similar incidents in the future?

- Are there any specific security measures that should be implemented based on this incident?

Activity 3: Microsoft Entra

Estimated time to complete this activity

20 minutes

Exercise 1: 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"

User	Risk state	Risk 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.

Exercise 2: Risky App Investigation

1. Go to the Entra portal (<https://entra.microsoft.com/>) and sign in with your credentials.
2. Click  on the top right side of the portal.

The screenshot shows the Microsoft Entra ID portal's 'Overview' page for a tenant named '(new) AlpineSkiHouse'. On the right side, the 'Copilot' feature is open with the prompt 'Show me unused apps'. The results pane lists 47 unused applications, each with a link to its details.

3. Try the following prompt "Show me unused apps"

The screenshot shows the Microsoft Entra ID portal's 'Overview' page for the same tenant. The 'Copilot' feature is open with the prompt 'Tell me more about the application app Id: fa5dde46-3c05-4cff-be94-3ac4e8778517'. The results pane displays detailed information about the application with the specified app ID, including its name, description, and other relevant details.

4. Try the following prompt "Tell me more about the application app Id: fa5dde46-3c05-4cff-be94-3ac4e8778517"

(new) AlpineSkiHouse

Basic information

- Name: (new) AlpineSkiHouse
- Tenant ID: 0527eb7-06fb-4769-b324-fd4a3bb865eb
- Primary domain: vnevado.alpineskihouse.co
- License: Microsoft Entra ID P2
- Users: 3,473
- Groups: 162
- Applications: 81
- Devices: 343

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

My feed

13beb513-a3c5-4bf2-a1c0-b39dc4085be Security Operator and 2 other roles View role information

Secure Score for Identity 69.87% Secure score updates can take up to 48 hours. View secure score

Copilot

- app: https://account.azure.com/appid: c0f042cc-c0a0-4488-web3-d365278562
- nevado.alpineskihouse-4fcf2c6b-4b55-49c7-9621-710e0f0f4aa - appid: 992ca106-1400-4e2f-af0d-429964e632e2
- adf-365-connector.ash - appid: 5df5ecf-39da-4e87-a268-4cfa182fe6fc

To verify this information and take remediation action in the Microsoft Entra admin center, you can navigate to the [Remove unused applications recommendation page](#) or the [Microsoft Entra admin center](#) and search for this application under 'Impacted Resources'.

Tell me more about the application app id: fa5dde46-3d05-4cff-be94-3ac4e8778517

Application Details

Display Name: DefenderAPIDemo

- ID: 1bcbb2ae-e3b4-4053-9640-ab99e77fa026
- App ID: fa5dde46-3d05-4cff-be94-3ac4e8778517
- Publisher Domain: vnevado.alpineskihouse.co
- Created Date/Time: 2024-08-01T06:30:42Z
- Sign-In Audience: AzureADMyOrg
- Verified Publisher: Not verified

To verify this information in the Microsoft Entra portal, you can navigate to the [App registrations page](#).

AI-generated content may be incorrect

Which permissions granted to this app?

Tell me more about these apps. Tell me more about applications in Entra.

Ask a question, search for info, or get help with a task in Security...

- Try the following prompt "Which permissions granted to this app ID: 14d82eec-204b-4c2f-b7e8-296a70dab67e are highly privileged?"

(new) AlpineSkiHouse

Basic information

- Name: (new) AlpineSkiHouse
- Tenant ID: 0527eb7-06fb-4769-b324-fd4a3bb865eb
- Primary domain: vnevado.alpineskihouse.co
- License: Microsoft Entra ID P2
- Users: 3,473
- Groups: 162
- Applications: 81
- Devices: 343

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

My feed

13beb513-a3c5-4bf2-a1c0-b39dc4085be Security Operator and 2 other roles View role information

Secure Score for Identity 69.87% Secure score updates can take up to 48 hours. View secure score

Copilot

- APP ID: 14d82eec-204b-4c2f-b7e8-296a70dab67e
- Publisher Domain: vnevado.alpineskihouse.co
- Created Date/Time: 2024-08-01T06:30:42Z
- Sign-In Audience: AzureADMyOrg
- Verified Publisher: Not verified

To verify this information in the Microsoft Entra portal, you can navigate to the [App registrations page](#).

AI-generated content may be incorrect

Which permissions granted to this app are highly privileged?

No highly privileged Application permissions were found. No highly privileged Entra Administrator roles were found. This data currently only looks at API permissions and Entra administrator (directory) roles. It doesn't look at non-directory permissions granted in places like Azure RBAC or other authorization systems.

To verify this information in the Microsoft Entra portal, you can navigate to the [Enterprise applications page](#).

AI-generated content may be incorrect

Which permissions granted to this app ID: 14d82eec-204b-4c2f-b7e8-296a70dab67e are highly privileged?

No highly privileged permissions were found for the application with App ID: 14d82eec-204b-4c2f-b7e8-296a70dab67e. To verify this information in the Microsoft Entra portal, you can navigate to the [Enterprise applications page](#).

AI-generated content may be incorrect

Ask a question, search for info, or get help with a task in Security...

Exercise 3: Entra Standalone

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 that has been flagged as a risky user.

⚠ 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: **Tell me about Entra user irvins@vnevado.alpineskihouse.co** in the prompt bar.
2. 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 Security Copilot, 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 4: Microsoft Purview

As a new compliance admin, you now have access to a vast array of data within the Purview products suite. Your job is to investigate DLP alerts using AI. Although you have strong experience with Symantec or another product, you're just starting to learn Microsoft Purview. You work for a large corporation handling sensitive data and complying with various regulations. Your role involves carefully reviewing documents to ensure all

procedures and policies are current and compliant. The following guidelines help to document how to begin your investigation within the Purview Products suite.

Assumptions

To proceed, we have the following assumptions in place:

1. Microsoft Purview Information Protection and Data Loss Prevention are set up to scan, label, and prevent data loss.
2. Insider Risk Management is set up along with Adaptive Protection.
3. Communication Compliance is set up and configured in the environment.
4. eDiscovery is being used and there are active cases.

Estimated time to complete this activity

30 minutes

Exercise 1: Microsoft Purview Data Loss Prevention

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.

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 about role-group permissions.](#)

Dot you know 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.

[View role groups](#) [Learn more about Incidents](#) [Go to Incidents page](#)

[Report](#) [Refresh](#)

Filter [Reset](#) [Filters](#)

Time range: 7/19/2024-8/19/2024 User: Any Alert status: Any Alert severity: Any

Alert name	Severity	Status	Time detected	Insider risk severity
DLP policy match for document 'SiteSecurityServiceState.txt' on a device	High	Active	Aug 18, 2024 10:41 AM	High
DLP policy match for email with subject 'Document'	Low	Active	Aug 14, 2024 10:02 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 'Project Obsidian document_Internal Only label.docx' on a device*".
4. Click on the *Summarize* -> "*Summarize alert*" at the bottom of the alert

Alert: DLP policy match for document 'Project Obsidian document_Internal Only label.docx' on a device

769e182a-ec34-478b-aa00-08dd25be6382

Alert status
Active

Alert severity
■■■ High

Time detected
Dec 27, 2024 11:31 AM

Number of events
1

DLP policy matched
Audit sharing of sensitive info with external collab sites

Locations
Devices

Users who performed the event

 u3932@ash.alpineskihouse.co

Assigned to
No one is assigned

Summarize alert Summarize user activity

View details Summarize ...

6. Alert summary will be generated

Alert: DLP policy match for document 'Project Obsidian document_Internal Only label.docx' on a device

Details Events User activity summary

Alert ID
769e182a-ec34-478b-aa00-08dd25be6382

Alert status
Active

Alert severity
High

Time detected
Dec 27, 2024 11:31 AM

Number of events
1

DLP policy matched
Audit sharing of sensitive info with external collab sites

Locations
Devices

Jan 17, 2025 4:48 PM ...

The high severity DLP alert with ID dl769e182a-ec34-478b-aa00-08dd25be6382 and Title "DLP policy (Audit sharing of sensitive info with external collab sites)" matched for document (Project Obsidian document_Internal Only label.docx) in a device was generated on December 26, 2024 15:02:00(UTC). The alert is currently in "new" status and is associated with the user u3932@ash.alpineskihouse.co.

The policy responsible for this alert is named "Audit sharing of sensitive info with external collab sites" with Policy ID 902979c5-cc91-43c7-a7fd-cc1f80d40fee. The rule that triggered the alert is "Audit upload to restricted apps and web sites" with Rule ID dfa1aeb3-6f28-45ca-8b11-edae6552dd6f0. This is related to the workload Endpoint.

Additionally, u3932@ash.alpineskihouse.co is marked as High risk level in Insider Risk Management.

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

What activity was performed on the data in this alert?

Describe the sensitive info, file labels, or data triggering this alert.

7. Next run the prompt "*Describe the sensitive info, file labels, or data triggering this alert*"
- This will return the information on users, devices, file and associated labels

Jan 17, 2025 4:53 PM

Describe the sensitive info, file labels, or data triggering this alert.

Jan 17, 2025 4:53 PM ...

Here is a summary of data at risk from Purview Information Protection and Data Loss Prevention because of alert dl769e182a-ec34-478b-aa00-08dd25be6382.

Users and Devices Involved:

UserPrincipalName	IRMRiskLevel
u3932@ash.alpineskihouse.co	High

Activity on Sensitive Files in the Past 7 Days:

FilePath
C:\Users\u3932\Downloads\OneDrive_2024-12-26\Demo sample files

Associated Files with Sensitive Info:

- C:\Users\u3932\Downloads\OneDrive_2024-12-26\Demo sample files\Project Obsidian document_Internal Only label.docx

7. Next run the prompt "*What activity was performed on the data in this alert?*" This will provide a summary of activities performed on the data related to this alert

Jan 17, 2025 5:01 PM

What activity was performed on the data in this alert?

Jan 17, 2025 5:01 PM ...

The activities performed on the data in this alert are as follows:

- DLPRuleMatch: 3 occurrences
- FileUploadedToCloud: 1 occurrence
- FileModified: 1 occurrence

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

gP ✓

8. We will now look at the user activity related to this alert. In the prompt enter '*Summarize user activity*' or you can navigate back to the alert view select *Summarize -> Summarize user activity*

Alert: DLP policy match for document 'Project Obsidian document_Internal Only label.docx' on a device

769e182a-ec34-478b-aa00-08dd25be6382

Alert status

Active

Alert severity

■■■ High

Time detected

Dec 27, 2024 11:31 AM

Number of events

1

DLP policy matched

Audit sharing of sensitive info with external collab sites

Locations

Devices

Users who performed the event

 u3932
u3932@ash.alpineskihouse.co

Assigned to

No one is assigned

Summarize alert

Summarize user activity

View details **Summarize** ...

The screenshot shows a summary of user activity for Jan 17, 2025 at 5:05 PM. It highlights that Microsoft Purview Insider Risk Management found details about User u3932. The summary includes:

- User Details:
 - User Name: u3932
 - Title:
 - User Principal Name: u3932@ash.alpineskihouse.co
- Insider Risk Severity: High
- Alert and case history: 0 active alerts and active case - Ash IRM Case
- User is in scope of 1 policies.
- Top Risk Factors based on user activities in the last 30 days:
 - User is found to be involved in Exfiltration activities. On December 26, 2024, they sent

- From the Alert, you can click on the View details to view the information related to the alert, using Copilot summary decreases the time needed to view and go through the full View Details page.

The screenshot shows the 'Details' tab of an alert for a DLP policy match. The alert ID is 769e182a-ec34-478b-aa00-08dd25be6382, and it is Active. The severity is High. The alert was detected on Dec 27, 2024 at 11:31 AM. There is 1 event. The DLP policy matched audit sharing of sensitive info with external collab sites. The location is a device, and the user who performed the event is u3932 (u3932@ash.alpineskihouse.co). A red box highlights the 'View details' button.

Exercise 2: Microsoft Purview 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 'Alerts' page within the Microsoft Purview Insider Risk Management solution. The left sidebar includes links for Overview, Recommendations, Alerts (selected), Cases, Policies, Users, Reports, Forensic Evidence, Notice templates, Audit log, Adaptive protection (preview), and Related solutions (Communication Compliance, Information Barriers, Data Loss Prevention). The main area displays a table of alerts with the following columns: ID, Created, Item, Policy, Status, Spotlight, Alert severity, Time detected, Assigned to, Case, and a delete icon. A search bar and filter options are at the top of the table. A message at the top states: "Priority user groups are not currently supported for use with Admin Units. It is recommended to ensure that the review of a priority user group are not restricted to specific admin units. Learn more about admin units." A 'Spotlight' section highlights one alert for 'isaiah'.

ID	Created	Item	Policy	Status	Spotlight	Alert severity	Time detected	Assigned to	Case	Delete
G7w64Df	2023-09-15 10:00:00	User Group	Date leak quick policy	Needs review	Low	2 days ago	Unassigned			
G411s60	2023-09-15 10:00:00	Ivan Belavich (OPB)	Project Objection	Needs review	High	4 days ago	Unassigned			
3bedcc7a	2023-09-15 10:00:00	Lisa Morris	Date leak quick policy	Needs review	High	11 days ago	Unassigned			
69a25c6d	2023-09-15 10:00:00	Nina Melny	Date leak quick policy	Needs review	Low	12 days ago	Unassigned			
a1600153	2023-09-15 10:00:00	Dalena Berger	Date leak quick policy	Needs review	Medium	12 days ago	Unassigned			
65be634	2023-09-15 10:00:00	Account Admin	Date leak quick policy	Needs review	High	13 days ago	Unassigned			

4. Choose the alert you want to review. For this example, please search "Isaiah" in the search bar and select the user. The following can be done with any IRM alert.

Alerts

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.](#)

ID	User	Policy	Status	Sophi...	Risk Level	Time detected	Assigned to	Case	Created
38f05eb	Isaiah Langer	Data leak quick poli...	Confirmed	■■■ High	4 months ago	Unassigned	Case 004: Potential d...	● Active	
a11b1bc	Isaiah Langer	Data leak quick poli...	Confirmed	■■■ High	5 months ago	Unassigned	Case 004: Potential d...	● Active	
c32004b	Isaiah Langer	Data leak quick poli...	Confirmed	■■■ High	6 months ago	Unassigned	Case 004: Potential d...	● Active	
b418f9b	Isaiah Langer	Data leak quick poli...	Confirmed	■■■ High	7 months ago	Unassigned	Case 004: Potential d...	● Active	
87a2151b	Isaiah Langer	Data leak quick poli...	Confirmed	■■■ High	a year ago	Unassigned	Case 004: Potential d...	● Active	
a77d1cb	Isaiah Langer	Project TNT - Alert	Confirmed	■■■ High	a year ago	Unassigned	Case 004: Potential d...	● Active	
bdb2847f	Isaiah Langer	Adaptive Protection p...	Confirmed	■■■ Medium	a year ago	Unassigned	Case 004: Potential d...	● Active	
5ef1f6b	Isaiah Langer	Project Christian	Confirmed	■■■ High	a year ago	Unassigned	Case 004: Potential d...	● Active	
<input checked="" type="checkbox"/> 86e52569	Isaiah Langer	Potential data theft - ...	Confirmed	■■■ High	a year ago	Unassigned	Case 004: Potential d...	● Active	

- Click on the *Summarize with Copilot* button below the User. This will provide details about the user, risk score, alert history and activities from the past 30 days

Isaiah Langer

Summarize with Copilot

User profile User activity

Name and title
 Isaiah Langer
 Marketing Analyst

Alert and activity summary
 User has 1 active alert, based on assigning risk scores to 5 activities.

User email
 isaiahl@vnevado.alpineskihouse.co

Alias
 isaiahl

Organization or department
 Marketing

Manager name
 Christie Cline

Manager email
 christiec@vnevado.alpineskihouse.co

Jan 17, 2025 5:20 PM ...

Microsoft Purview Insider Risk Management found the following details about User Isaiah Langer:

- User Details
 - User Name: Isaiah Langer
 - Title: Marketing Analyst
 - User Principal Name: isaiahl@vnevado.alpineskihouse.co
- Insider Risk Severity: Low
- Alert and case history: 1 active alert
- User is in scope of 1 policy.
- Top Risk Factors based on user activities in the last 30 days:
 - Exfiltration (December 21, 2024(UTC)) - User is found to be sending emails with attachments outside the organization 1 time. The emails contained 1 total email and was shared with 1 recipient.

To get a detailed view of Isaiah Langer's activities, you can visit: [View all activity](#)

- From the Copilot prompt, click on the book icon and review the list of available prompts, select any prompt to dive deeper into user activity, you can select any recommended prompts from the list. In the example below, we'll run "Did the user engage in any unusual behavior?" and "Summarize user's last 30 days of activity" and review the results.

The screenshot shows the Microsoft Copilot interface for a user named Isaiah Langer. On the left, there is a sidebar with user profile information: Name and title (Isaiah Langer, Marketing Analyst), Alert and activity summary (1 active alert, 5 activities), User email (isaiahl@vnevado.alpineskihouse.co), Alias (isaiahl), Organization or department (Marketing), Manager name (Christie Cline), Manager email (christiec@vnevado.alpineskihouse.co), and In scope. The main area is titled "Copilot Preview" and contains a message from "IRMUserLink" stating "AI-generated content may be incorrect. Check it for accuracy." Below this is a timestamp "Jan 17, 2025 5:23 PM" and a prompt: "Did the user engage in any unusual behavior?". To the right of this prompt is a list of suggested actions: "List the data exfiltration activities involving this user.", "List sequential activities involving this user", and "Show key actions performed by the user in the last 10 days.". Further down are additional prompts: "summarize user's last 30 days of activity.", "List all the data exfiltration activities involving this user.", and "List all the sequential activities involving this user.". At the bottom of the list is another prompt: "Did the user engage in any unusual behavior?", which has a red box around it. A red box also highlights the "summarize user's last 30 days of activity." prompt at the bottom of the list. A red square box is drawn around the entire list of prompts.

Exercise 4: Microsoft Purview Communication Compliance

Reviewing communication violations, particularly for extensive content like meeting transcripts, email attachments, Teams attachments, or lengthy texts, can be quite time-consuming. As a compliance administrator monitoring the sharing of unauthorized information, you need an efficient method for conducting initial investigations. Rather than reading each transcript manually to identify violations, you can leverage the Copilot integration to assist you. There have been several meetings concerning stock, and it is crucial to verify that these meetings complied with organizational standards. Follow the subsequent steps to identify any violations without needing to read through each individual transcript.

Step-by-Step Guidance

1. Go to the new Purview Portal (<https://purview.microsoft.com>) and sign in with your credentials. Select Communication compliance.
2. Navigate to Policies and select Regulatory Compliance.

The screenshot shows the Microsoft Purview Policies page. On the left, there's a sidebar with 'Communication Compliance' selected. The main area has tabs for 'Policy warnings' (0), 'Policy recommendations' (4), and 'Healthy policies' (14). A message at the top says 'Some user reported messages contain workplace safety violations. Open the policy to view the potentially risky content. The "User-reported messages" policy was automatically created by Microsoft to detect Teams and Viva Engage messages that users reported as inappropriate.' Below this are buttons for 'Open policy' and 'Create Inappropriate Content policy'. The main table lists 18 policies with columns for Policy name, Messages scanned today, New pending to..., Total pending, Total resolved, Status, and Policy health. The 'Regulatory compliance' policy is checked in the first row.

Policy name	Messages scanned today	New pending to...	Total pending	Total resolved	Status	Policy health
Regulatory compliance	0	0	133	90	Active	Healthy
Inappropriate Text - Test	0	0	0	0	Active	Healthy
Insider risk trigger 24-01	0	0	0	0	Active	1 recommendation
Insider risk indicator 24-01	0	0	115	9	Active	Healthy
New Inappropriate Text	0	0	0	0	Active	Healthy
Bulk_Teg_test	0	0	0	9565	Active	Healthy
AI hub - Unethical behav	0	0	24	6	Active	Healthy
full names and addresse	0	0	3254	18706	Paused	Healthy
Inappropriate Content	0	0	0	9728	Active	1 recommendation
Conflict of interest - sal	0	0	0	0	Active	Healthy
Secrets and passwords	0	0	132	208	Active	Healthy
Confidential proj	0	0	246	3684	Active	Healthy
Inappropriate Content C	0	0	0	9741	Active	1 recommendation
Copilot for Microsoft 36	0	0	3	225	Active	Healthy
User-reported message	0	0	5	0	Active	Healthy
Project Woodgrove	0	0	35	6796	Active	Healthy
Regulatory compliance	0	0	59	2437	Active	Healthy
Inappropriate Images	0	0	0	16	Active	1 recommendation

3. Click on a policy match to view message content. Search “stock” in the Body/Subject filter and select the Stock meeting. You’re able to choose any Teams meeting to get a similar experience.

The screenshot shows the Microsoft Communication Compliance interface. On the left, there's a sidebar with 'Communication Compliance' at the top, followed by 'Overview', 'Policies', 'Alerts', 'Reports', and 'Classifiers'. Below that is a 'Related solutions' section with 'Information Barriers' and 'Insider Risk Management'. The main area is titled 'Regulatory compliance' and shows a search bar with 'Body/Subject: stock'. It displays a list of 28 selected items, with one item highlighted: 'Stock meeting' (Copilot in BizChat). To the right of the list is a detailed view of this item, including a 'Summary' tab (selected) and a 'User history' tab. The summary includes a warning message: 'Conditions detected: Stock manipulation (stock is going to skyrocket, +1 more). Unauthorized disclosure (not disclose t...)' and a link to 'Review meeting transcripts'. Below the summary are sections for 'Meeting info' (Sender (From), Start time, End time, Recipient (To), Subject), and a 'Details' section with a 'QUESTIONABLE' status. At the bottom are buttons for 'Resolve', 'Summarize', 'Notify', 'Tag as', 'Escalate', and 'Automate'.

4. Click on Summarize (NOTE: Contextual summaries are only eligible for messages and attachments with a combined length of 100 words or more.)

The screenshot shows the Microsoft Purview Communication Compliance interface. On the left, there's a sidebar with 'Communication Compliance' selected, followed by 'Overview', 'Policies', 'Alerts', 'Reports', and 'Classifiers'. Below these are 'Related solutions' like 'Information Barriers' and 'Insider Risk Management'. The main area is titled 'Policies > Regulatory compliance' and shows 'Pending (59)', 'Resolved (2437)', and 'Exports' buttons. A search bar at the top right has 'Search' and a 'Copilot' button. The main content area displays a list of messages under 'Body/Subject: stock'. One message is expanded, titled 'Stock meeting'. It includes sections for 'Summary', 'User history', and 'Review meeting transcripts'. The 'Meeting info' section shows details like 'Sender (From)', 'Start time', 'End time', 'Recipient (To)', and 'Subject'. To the right, a 'Copilot' window provides a summary of the detected conditions: 'Stock manipulation' and 'Unauthorized disclosure'. It also includes a note about Microsoft's stock price and a warning about keeping information confidential. Buttons at the bottom include 'Resolve', 'Summarize', 'Notify', 'Tag as', 'Escalate', and 'Automate'.

- To learn more about the meeting, explore additional default prompts or type your own question into the text prompt. An example could be regarding the people involved in the message.

Communication Compliance

Overview Policies Alerts Reports Classifiers

Policies > Regulatory compliance

Pending (59) Resolved (2437) Exports

Filter Reset Filters

Body/Subject: stock Date: Any Sender: Any Tags: Any

1 of 28 selected

Stock meeting

Summary User history

⚠ Conditions detected: Stock manipulation (stock is going to skyrocket, +1 more), Unauthorized disclosure

Review meeting transcripts

To review transcripts, expand this item in the list and select the transcript you want to review.

Meeting info

Sender (From) padavid@woodgrove.ms <padavid@woodgrove.ms>

Start time Tue Jan 16 2024 13:42:57 GMT-0800

End time Tue Jan 16 2024 13:44:14 GMT-0800

Recipient (To) chrisfie@woodgrove.ms <chrisfie@woodgrove.ms>; jenli@woodgrove.ms <jenli@woodgrove.ms>; padavid@woodgrove.ms <padavid@woodgrove.ms>

Subject Stock meeting

Stock action

Copilot in BioChat

Stock meeting

yo

Copilot in BioChat

They're coming out with Q1 numbers here and next week, and I've already seen the numbers.' and 'Let's not disclose this information to anyone under any circumstances. Please keep this information confidential.'

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

What content in the message was flagged as Stock manipulation and Unauthorized disclosure categories?

Copilot

Aug 19, 2024, 2:12 PM

The content of the message contains instances that fall under the categories of 'Stock manipulation' and 'Unauthorized disclosure'.

In the context of 'Stock manipulation': the statement 'They're coming out with Q1 numbers here and next week, and I've already seen the numbers. These numbers are just amazing. We should really buy this stock' suggests an attempt to influence the stock price.

Regarding 'Unauthorized disclosure', the phrases 'Let's not disclose this information to anyone under any circumstances. Please keep this information confidential.' and 'I've already seen the numbers.' indicate the sharing of confidential or internal content with someone outside the designated group.

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

Generate a simple summary of this message

Ask a question or get more insights about the selected message.

0/500 ➤

Exercise 4: Microsoft Purview eDiscovery

Scenario 1: Gain summary of a eDiscovery case review set

1. Open the case titled “Alpine stock manipulation” and then the Review Set, “Stock Manipulation.” This will work with any review set within a case

Scenario 1: Generate an eDiscovery search query with Security Copilot

1. Navigate to the new Purview portal (purview.microsoft.com) and go to the Cases subsection under eDiscovery.

Cases								
	Create case	Download list	Refresh	119 items	Filter by keyword	Filter	Group	Customize columns
	Name	Case status	Case type	Created on	Last modified	Last modified by	Number	
1	Test Case 1	Active	Premium	Aug 13, 2024 10:29 AM	Aug 13, 2024 10:30 AM	Sophie Davis	1	
2	Test search for CTI	Active	Premium	Aug 13, 2024 9:36 AM	Aug 13, 2024 9:36 AM	Ryan Martinez	2	
3	MNGO - Mark 8 Project Investigation	Active	Premium	Aug 13, 2024 9:22 AM	Aug 13, 2024 9:22 AM	Dean Hernandez	3	
4	New SQL search for excluding internal...	Active	Premium	Aug 12, 2024 1:25 PM	Aug 12, 2024 1:25 PM	Elizabeth Amato	4	
5	Test Case 12	Active	Premium	Aug 9, 2024 9:31 AM	Aug 9, 2024 9:31 AM	Ariat Burke	5	
6	CT2024 - Woodgrove Sales	Active	Premium	Aug 9, 2024 1:23 AM	Aug 9, 2024 1:23 AM	Ariat Burke	6	
7	CT2024 - Arash Burke Collection	Active	Premium	Aug 8, 2024 8:11 AM	Aug 8, 2024 8:11 AM	Ariat Burke	7	
8	SDAN-TEST0000	Active	Premium	Aug 7, 2024 9:49 PM	Aug 7, 2024 9:49 PM	Madeline Hartman	8	
9	CT2024 - Contracts vs Woodgrove	Active	Premium	Aug 7, 2024 9:34 AM	Aug 7, 2024 9:34 AM	Ariat Burke	9	
10	secreta_davis	Active	Premium	Aug 7, 2024 7:46 AM	Aug 7, 2024 7:46 AM	Madeline Hartman	10	
11	CT2024 - HR Contracts	Active	Standard	Aug 7, 2024 1:48 AM	Aug 7, 2024 1:48 AM	Ariat Burke	11	
12	Test for external email ID	Active	Premium	Aug 6, 2024 1:03 PM	Aug 6, 2024 1:03 PM	Elizabeth Amato	12	
13	Bug Test	Active	Premium	Aug 6, 2024 10:12 AM	Aug 6, 2024 10:12 AM	Ariat Burke	13	
14	Iya Bharatari Sample Case 1	Active	Premium	Aug 6, 2024 10:10 AM	Aug 6, 2024 10:10 AM	Iya Bharatari	14	
15	External and Internal email tracking	Active	Premium	Aug 6, 2024 10:01 AM	Aug 6, 2024 10:01 AM	Elizabeth Amato	15	
16	Test case	Active	Standard	Aug 6, 2024 9:34 AM	Aug 6, 2024 9:34 AM	Elizabeth Amato	16	

2. Navigate to an eDiscovery case. Then navigate to searches. Click Create a search. Give it a name and select Create.

The screenshot shows the Microsoft eDiscovery interface. On the left, there's a sidebar with options like Home, Overview, Cases, Audit, and Related solutions. The main area is titled "M002a - Mark 8 Project Investigation". It shows a list of search items:

Name	Description	Query text	Created by	Created date	Last modified by	Last modified
5003 - DUGO Mark 8 state collection (EDR)	EDR Mark 8 state collection (EDR)	(Date>2023-09-17)	dugo10@contoso.com	Aug 11, 2024 5:17...	dugo10@contoso.com	Aug 11, 2024 5:17...
5004 - Rely Mark 8 state collection	Rely Mark 8 state collection	(Date>2024-09-12)	dugo10@contoso.com	Aug 11, 2024 5:17...	dugo10@contoso.com	Aug 11, 2024 5:17...
5001a - Initial Mark 8 state-range collection (C7, CA, HTML)	Initial Mark 8 state-range collection (C7, CA, HTML)	(Date>2024-08-18)	dugo10@contoso.com	Aug 11, 2024 5:26...	dugo10@contoso.com	Aug 11, 2024 5:26...

3. Click “Draft with Security Copilot”

The screenshot shows the Microsoft eDiscovery interface with the "Project Investigation" search query builder. The left sidebar has "eDiscovery" selected. The main area shows the search query configuration:

- Query: "Draft a query with Copilot"
- Data sources: Synced
- Condition builder: AND (Select a filter)
- Keyword query language (KeyQL): Search

4. Provide your own natural language input or select one of the suggested prompts. In this case, we will use the following: “Find all the emails that have the words confidential, and budget attached in November 2023. List all the users associated with that email.”

Project Investigation

Add to review set Export Process manager

Query:

Query Statistics Sample

Draft a query with Copilot

Natural language prompt

Start by entering your search query including user, data source and content details.

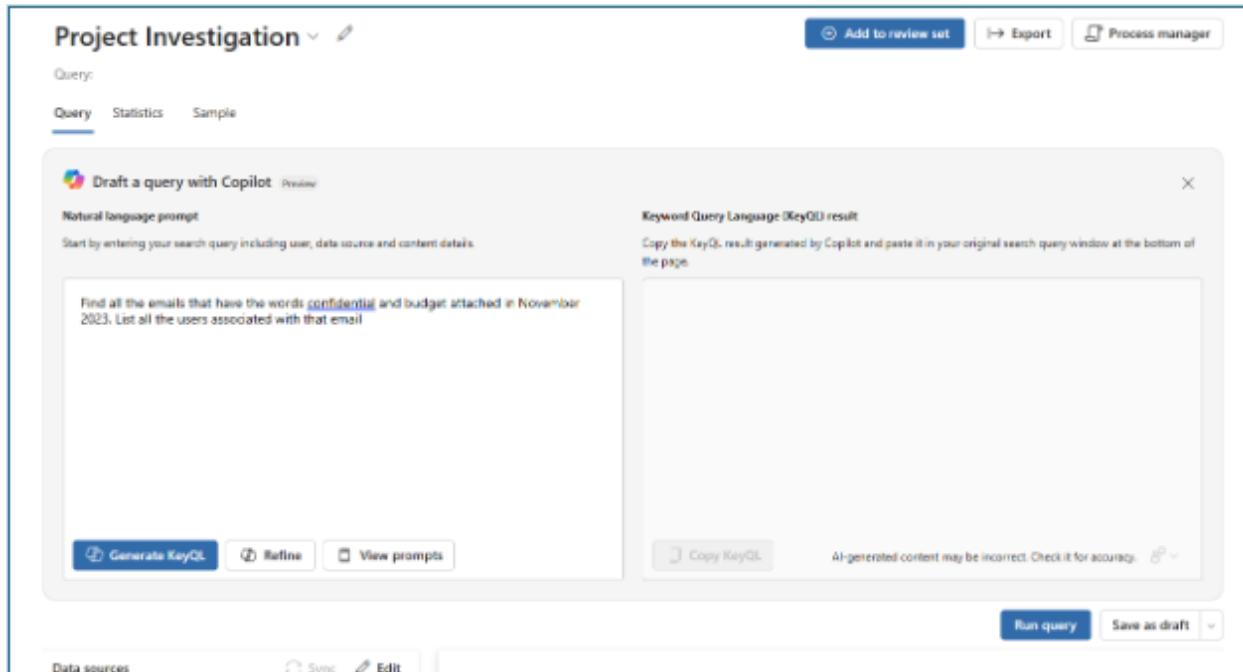
Find all the emails that have the words **confidential** and budget attached in November 2023. List all the users associated with that email

Generate KeyQL Refine View prompts

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

Run query Save as draft

Data sources Sync Edit



- Click “Refine” to optimize your natural language input for Security Copilot. Either accept or discard the suggested refinement.

Project Investigation

Add to review set Export Process manager

Query:

Query Statistics Sample

Draft a query with Copilot

Natural language prompt

Start by entering your search query including user, data source and content details.

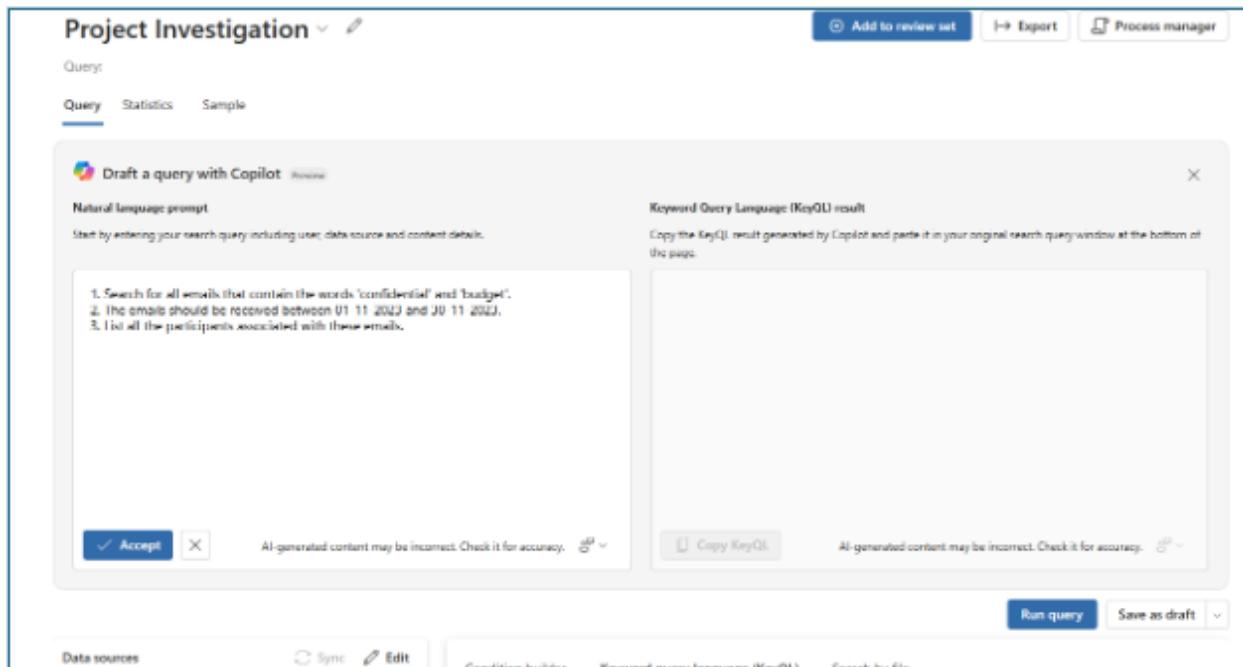
1. Search for all emails that contain the words 'confidential' and 'budget'.
2. The emails should be received between 01/11/2023 and 30/11/2023.
3. List all the participants associated with these emails.

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

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

Run query Save as draft

Data sources Sync Edit



- Click “Generate KQL” to generate a search query from the natural language input.

The screenshot shows the Project Investigation interface. At the top, there are buttons for 'Add to review set', 'Export', and 'Process manager'. Below that, a 'Query' section has tabs for 'Query' (which is selected), 'Statistics', and 'Sample'. A modal window titled 'Draft a query with Copilot' is open. It contains a 'Natural language prompt' field with placeholder text: 'Start by entering your search query including user, data source and content details.' Below this is a list of three items: '1. Search for all emails that contain the words "confidential" and "budget".', '2. The emails should be received between 01-11-2023 and 30-11-2023.', and '3. List all the participants associated with these emails.' To the right of the prompt is a 'Keyword Query Language (KeyQL) result' section containing the generated KQL: '(("confidential" AND "budget") AND ((received>="2023-11-01") AND (received<="2023-11-30")))'.

7. Click “Copy KQL” to copy the KQL result generated by Copilot and paste it in your original search query window at the bottom of the page.

X

Keyword Query Language (KeyQL) result

Copy the KeyQL result generated by Copilot and paste it in your original search query window at the bottom of the page.

```
(("confidential" AND "budget") AND ((received>="2023-11-01") AND (received<="2023-11-30")))
```

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

Condition builder Keyword query language (KeyQL) Search by file

```
(("confidential" AND "budget") AND ((received>="2023-11-01") AND (received<="2023-11-30")))
```

0 errors detected

8. To run the query copied from previous step, paste in the Condition builder, add data source or add tenant-wide source and click Run query

The screenshot shows the Microsoft Purview Query interface. At the top, there are tabs for 'Query', 'Statistics', and 'Sample'. Below the tabs, there are buttons for 'Summarize this search' and 'Draft a query with Copilot'. On the right side, there are buttons for 'Run query' and 'Save as draft'. The main area is titled 'Condition builder' with a sub-instruction: 'Build a search query with a visual condition filtering experience. To create a query with conditional filtering, use operators like AND/OR and other controls. To use a query language, copy and paste KeyQL into the builder or add it as a value. Learn more about condition builder'. A search bar labeled 'Search by file' is present. The query editor shows a condition: 'KeyQL Equal ((subject:"confidential") AND (subject:"budget") AND ((received>="2023-11-01") AND (received<="2023-12-01") OR (sent>="2023-11-01") AND (sent<="2023-12-01"))'. Below the editor, it says '0 errors detected'. At the bottom left, there are buttons for 'Add sources' and 'Add tenant-wide sources'. A note on the left says: 'Get started by adding data sources to your search query. To search across your entire organization or tenant, select Add tenant-wide sources. Learn more about sources'.

Exercise 5: Microsoft Purview Data Security Posture Management (DSPM)

Data security administrators can leverage Copilot for Security in DSPM to delve deeper into dashboard insights and conduct critical data security investigations. With Copilot, you can quickly uncover insights across various dimensions such as activities, files, devices, users, departments, or regions, enabling you to manage your data security posture more effectively.

Step-by-Step Guidance: Start using Copilot in DSPM

1. Go to the purview portal - <https://purview.microsoft.com/> and sign in with your credentials.
2. Navigate to solutions -> Data Security Posture Management
3. We have provided starter prompts to get you quickly started with Copilot-

The screenshot shows the Microsoft Purview Data Security Posture Management (preview) dashboard. The left sidebar includes icons for Home, Solutions, IP, User, Settings, and a dropdown for 'Microsoft Purview'. The main content area is titled 'Data Security Posture Management (preview)' with a sub-instruction: 'Get insights and recommendations for protecting sensitive data. Improving security posture will minimize risks using Security Copilot. Learn more about Data Security Posture Management'. Below this, there are four cards: 'Priority alerts' (which alerts were triggered in the last 30 days for users leaving the org), 'Detect sensitive file leaks' (which sensitive files were shared outside the org from SharePoint in the last week), 'Find devices at risk' (which devices were involved in malicious activities), and 'Find risky activity' (any suspicious activity sequences involving sensitive data).

4. You can also access Security Copilot from the Purview header by clicking on the copilot icon and entering your prompt. Given below are some sample prompts:
 - Provide details of the file and user for events where files labeled as highly confidential were copied to the network share in the past two days.
 - Display all activities performed on the file located at <full file path> in the past two days.

- Display all activities done by user jDoe@company.com that involved priority content.
- Show me all the users who copied sensitive data to USB in the last 10 days.
- List all the devices that were involved in an exfiltration activity.
- Display the top 5 users with the most exfiltration activities in the last 30 days.

The screenshot shows the Microsoft Copilot interface within the Data Security Posture Management (DSPM) preview. The main dashboard features several cards for 'Get started with Copilot' (Priority alerts, Detect sensitive data leaks, Red devices at risk, Red risky activity), 'Top data security risk recommendations' (Mitigate potential risks with adaptive protection, Prevent sequential activities that might leak sensitive data), and 'Analytics reports' (Unprotected sensitive assets across data sources, Users performing top exfiltration activities involving sensitive assets). On the right side, there is a sidebar titled 'Copilot tasks' which lists specific activities performed by users related to Project Obsidian, such as files shared externally from SharePoint and OneDrive. The sidebar also includes a note about generating content being inferred and links to more details on specific activities.

5. Experiment with different prompts and variations to see what works best for your use case. Chat AI models vary, so iterate and refine your prompts based on the results you receive.
6. Use the feedback within Copilot to tell us if the responses are accurate or not.
7. For more information on writing Security Copilot prompts, go to [Microsoft Security Copilot prompting tips](#). For an enhanced experience with Copilot in DSPM, we recommend adhering to the following guidelines-
 - Questions involving a certain user should always include the user's UPN.
 - Questions involving a certain type of sensitive info type or label should specify the complete name for the sensitive info type or label for higher accuracy in response.
 - Questions where you want to get some top users/activities/alerts etc. should clearly list the sorting criteria for higher accuracy in response.

- Questions where you're looking for data in a certain timeframe, please specify that timeframe because by default we will look back to only 10 days. The max. lookback we can support is 30 days
- Entities (OOB/Custom SITs/TC/Label) to be put in single quotes in prompt
- Any path (eg. file path) mentioned in the user prompt must use "/" as separator, NOT "\".
- The accuracy of response will be higher if it's asking a single intent. If user has a complex question, it is advised that user should break it into single intent questions, and ask it one by one (sequentially)
- User questions should be self-contained. For higher accuracy, avoid giving reference to previous questions or response.
- Avoid using generic terms, user questions with product specific terms will have higher accuracy.
- You can ask questions about data security across information protection, data loss prevention and insider risk management or get a summary from public documentation.

Exercise 6: Microsoft Purview DLP Policy Insights with Copilot

Scope of this feature: Administrators can invoke the policy insights skill to understand, comprehend the insights from all their policies or a handful of selected policies. The insights offered start with a higher-level view of how their policies:

- are effective across locations,
- detect the presence of what sensitive information types throughout their digital estate
- how administrators are notified of violations
- how users are educated while they perform activities they should not

These insights are offered with different pivots by location, classification and by administrative scopes. This is offered to give the security policy administrators different views for deeper understanding of policy constructs and their impact.

Step-by-Step Guidance: Gain DLP Policy Insights with Copilot

1. Select the policies you wish to get insights/quick summary on

The screenshot shows the Microsoft Purview Data Loss Prevention Policies page. On the left, there's a sidebar with navigation links like Home, Data Loss Prevention (selected), Overview, Policies (selected), Alerts, Activity explorer, Classifiers, Explorers, and Related solutions. The main content area has a title 'Policies' and a message about devices being in an updated state. Below that is a table titled 'Get insights with Copilot' showing 2 of 23 selected policies. The table columns are Name, Priority, Last modified, and Status. Policies listed include 'Sensitive file exfiltration from endpoint', 'DLP Policy - Classified Project Files on Windows Devi...', 'U.S. Financial Data', and 'DLP Policy - Classified Project Documents'. A Copilot sidebar on the right shows a history of interactions and a prompt to ask a question about DLP policies.

- Click on the Get Insights with Copilot button. You will see the prompt is already pushed into the copilot experience in the side panel.

This screenshot is similar to the previous one but shows the Copilot sidebar more prominently. The sidebar includes a 'Copilot Preview' section with troubleshooting tips for DLP, a 'Generating...' status bar, and a text input field asking for a specific question about Microsoft Purview documentation.

- Copilot responds with insights on the selected policies

The screenshot shows the Microsoft Purview Data Loss Prevention Policies page on the left and the Microsoft Security Copilot interface on the right.

Purview Policies Page:

- Left sidebar: Home, Data Loss Prevention (selected), Learn, Policies (selected), Alerts, Activity explorer, Classifiers, Explorers, Related solutions (Information Protection, Insider Risk Management).
- Main area: A message about role group permissions, a search bar, and a table titled "Get insights with Copilot" showing 2 of 23 selected policies. The table columns are Name, Priority, and Last modified. Policies listed include "Sensitive file exfiltration from endpoint", "DLP Policy - Classified Project Files on Wind...", "U.S. Financial Data", "DLP Policy - Classified Project Documents", "Adaptive Protection policy for Endpoint DLP", "Adaptive Protection policy for Teams and Exch...", "Project Obsidian DLP", "Block restricted content from USB drives", "Block upload to third party cloud services", and "Avoid Sharing of PAN and AADHAR".

Copilot Interface:

- Top bar: Search, New Microsoft Purview portal, Copilot icon.
- Message card: Nov 18, 2024 10:05 AM, "Give me insights on my DLP policies".
- Text area: "As per the policy you have selected, here are the insights on your DLP policies: Where are your policies looking for data? Your policies are applied to data stored in the following locations:" followed by a bulleted list: SharePoint (2 policies), OneDrive for Business (2 policies), Exchange (2 policies), Teams (2 policies), Endpoint Devices (1 policy), Third Party Apps (1 policy).
- Input fields: "What specific types of sensitive information does this DLP policy aim to protect?", "What types of sensitive information are we protecting with these DLP policies?", and "Ask a specific question about a topic in Microsoft Purview documentation".
- Bottom right: "0 / 2000" and a send button.

Exercise 7: Microsoft Purview Standalone

To start your investigation, ensure you gather data from Purview and other integrations within the suite. Instead of individually visiting Entra, DLP, and other locations, try the Standalone investigation experience with Microsoft Security Copilot. Follow the instructions below to set up Microsoft Security Copilot for Purview.

1. Login to Security Copilot [<https://securitycopilot.microsoft.com>] and sign in with your credentials.
2. Start a new session and enter the following prompts

Please follow the prompts below to do a Microsoft Purview Data Loss Prevention Investigation using the Standalone experience:

- *Which Purview Data Loss Prevention alerts should I prioritize today?*

Which Purview Data Loss Prevention alerts should I prioritize today?

> 3 steps completed 59 seconds

Aug 19, 12:23 PM

Displaying top 10 Microsoft Purview Data Loss Prevention (DLP) alerts with status 'New' and 'High' severity:

Alert ID	Alert Name	Severity
dl9c19b080-af20-71aa-0c00-08dcbe1a2c37	DLP policy (AP - Block Cloud and USB) matched for document (SiteSecurityServiceState.txt) in a device	High
	DLP policy (AP - Block Cloud)	

Export to Excel

- Can you summarize the first purview alert?

Can you summarize the first purview alert?

> 3 steps completed 32 seconds

Aug 19, 12:25 PM

The high severity DLP alert with ID `dl9c19b080-af20-71aa-0c00-08dcbe1a2c37` and title "DLP policy (AP - Block Cloud and USB) matched for document (SiteSecurityServiceState.txt) in a device" was generated on August 16, 2024 at 17:37:00 (UTC). The alert is currently in "new" status and is associated with the user `natala.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".

The device involved in this alert has the ID `8d41c164b10e77fd0058ad964c20fb2f2087c4ec`.

Additionally, `Natala.David_0716@woodgrove.ms` is marked as high risk level in Insider Risk Management.

- What was the data or action that triggered this alert?

What was the data or action that triggered this alert?

> 3 steps completed 38 seconds

Aug 19, 12:27 PM

The alert was triggered by the following activities and data:

1. Users and Devices Involved:

User Principal Name	Insider Risk Level	Device ID
natasha.david_0716@woodgrove.ms	High	8d41c164b10e77fd0058ad964c 20fb2f2087c4ec

2. Sensitive File Path Occurrence:

File Path	Occurrence
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\SiteSecurityServiceState.txt	1

3. Associated Files:

File
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\SiteSecurityServiceState.txt

4. Activities Found on This Data:

Activity	Count
DLPRuleMatch	3
FileAccessedByUnallowedApp	2
FileRenamed	1
FileCopiedToClipboard	1

The user `natasha.david_0716@woodgrove.ms` accessed the file `SiteSecurityServiceState.txt` located at `C:\\\\Users\\\\NatashaDavid(TA)\\\\OneDrive - Woodgrove\\\\Desktop\\\\Tor Browser\\\\Browser\\\\TorBrowser\\\\Data\\\\Browser\\\\profile.default`. The activities performed on this file include matching a DLP rule 3 times, accessing the file by an unallowed app 2 times, renaming the file once, and copying the file to the clipboard once.

- *What are the data risks related to this alert?*

What are the data risks related to this alert?

> **3 steps completed** 58 seconds

Aug 19, 12:29 PM

The data risks associated with the alert `d19c19b080-af20-71aa-0c00-08dcb1a2c37` are as follows:

1. Users and Devices Involved:

User Principal Name	Insider Risk Level	Device ID
natasha.david_0716@woodgrove.ms	High	8d41c164b10e77fd0058ad964c 20fb2f2087c4ec

2. Sensitive File Path Occurrence:

File Path	Occurrence
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default	1

3. Associated Files:

File
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\SiteSecurityServiceState.txt

4. Activities Found on This Data:

Activity	Count
DLPRuleMatch	3
FileAccessedByUnallowedApp	2
FileRenamed	1
FileCopiedToClipboard	1

The user `natasha.david_0716@woodgrove.ms` accessed the file `SiteSecurityServiceState.txt` located at `C:\\\\Users\\\\NatashaDavid(TA)\\\\OneDrive - Woodgrove\\\\Desktop\\\\Tor Browser\\\\Browser\\\\TorBrowser\\\\Data\\\\Browser\\\\profile.default`. The activities performed on this file include matching a DLP rule 3 times, accessing the file by an unallowed app 2 times, renaming the file once, and copying the file to the clipboard once. These activities pose a risk as they involve a sensitive file and were performed by a user with a high insider risk level.

- For the files related to the alert, show me all activities done in the last 7 days?
NOTE: This depends on if files were impacted.

For the files related to the alert, show me all activities done in last 7 days?

> ✓ 3 steps completed 53 seconds

Aug 19, 12:31 PM

In the last 7 days, the following activities were performed on the file `siteSecurityservicestate.txt`:

Activity	Count
DLPRuleMatch	3
FileAccessedByUnallowedApp	2
FileRenamed	1
FileCopiedToClipboard	1

Export to Excel 🔗

These activities indicate that the file was accessed by an unallowed application, copied to the clipboard, renamed, and matched a DLP rule multiple times. This could potentially indicate a data breach or misuse of sensitive information.

- *What Suspicious Actions Have Been Performed On This File? NOTE: this depends on if files were impacted.*

What Suspicious Actions Have Been Performed On This File?

< ✓ 3 steps completed 57 seconds

> ✓ Chose Microsoft Purview 26 seconds

> ✓ Retrieved data risk information. 22 seconds

> ✓ Prepared your response 9 seconds

Aug 19, 12:35 PM

In the last 7 days, the following suspicious activities were performed on the file `siteSecurityserviceState.txt`:

- The DLP rule was matched 3 times.
- The file was accessed by an unallowed application 2 times.
- The file was copied to the clipboard once.
- The file was renamed once.

These activities indicate potential misuse or unauthorized access to sensitive data.

🔗 How's this response? ↓ □

- *According to Purview, What is the implication of these DLP Alerts?*

According to Purview, What is the implication of these DLP Alerts?

> 3 steps completed 39 seconds

[uft.com\] is signed in](#)
Aug 19, 12:38 PM

Here is a summary of data at risk from Purview Information Protection and Data Loss Prevention because of alert `d19c19b080-af20-71aa-0c00-08dcbe1a2c37`.

This involves the following users and devices:

User Principal Name	Insider Risk Level	Device ID
natasha.david_0716@woodgrove.ms	High	8d41c164b10e77fd0058ad964c 20fb2f2087c4ec

The activity performed on the files with sensitive info by these users (found on these devices) in the past 7 days is as follows:

File Path	Occurrence
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\SiteSecurityServiceState.txt	1

The associated files with sensitive info are as follows:

File
C:\Users\NatashaDavid(TA)\OneDrive - Woodgrove\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\SiteSecurityServiceState.txt

Activities found on this data:

Activity	Count
DLPRuleMatch	3
FileAccessedByUnallowedApp	2
FileCopiedToClipboard	1
FileRenamed	1

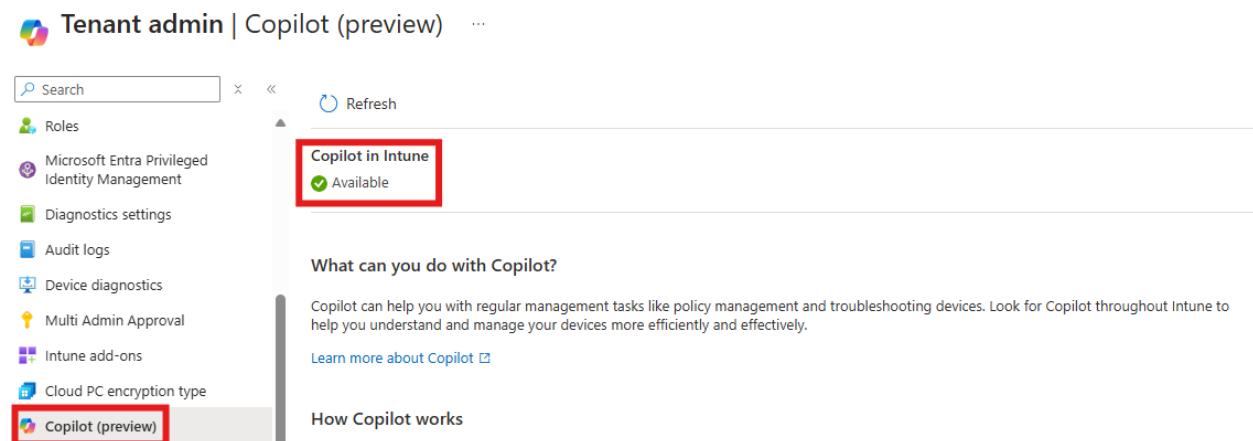
These activities indicate potential misuse or unauthorized access to sensitive data.

Be clear and specific with your prompts. Prompts are improved if **Purview** is added, example: **According to Purview, what is the risk associated with this user.**

Activity 5: Intune

This activity will give you hands-on experience with the Copilot in Intune capabilities embedded natively within Microsoft Intune. Copilot technology assists the IT/Device administrators in areas like managing policies and settings, understanding security posture, and troubleshooting of device issues.

Confirm Copilot is enabled in Intune - Using your Alpine Skihouse account, login into <https://intune.microsoft.com> > **Tenant administration** > **Copilot**.



The screenshot shows the Microsoft Intune Tenant admin interface. The left sidebar has several items: Roles, Microsoft Entra Privileged Identity Management, Diagnostics settings, Audit logs, Device diagnostics, Multi Admin Approval, Intune add-ons, Cloud PC encryption type, and Copilot (preview). The 'Copilot (preview)' item is highlighted with a red box. The main content area shows a 'Copilot in Intune' section with a green checkmark and the word 'Available'. Below it is a 'What can you do with Copilot?' section with a brief description and a 'Learn more about Copilot' link. At the bottom is a 'How Copilot works' section.

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

Estimated time to complete this activity

20 minutes

Exercise 1: Policy Management – Setting Information, understanding Policy settings Conflicts and User and Security Impact Assessment

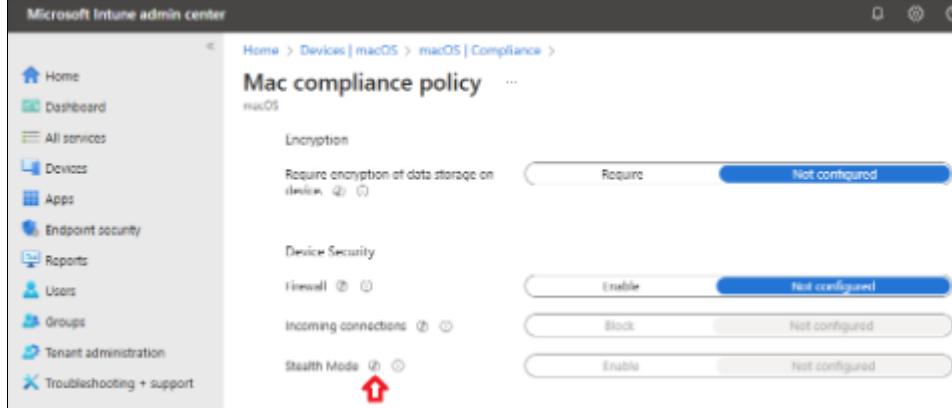
You are an IT admin responsible for ensuring that the Intune environment has the right set of device management policies to meet your organization's business requirements.

You have been asked to ensure that macOS devices meet a base level of security before they are able to access corporate resources. To do this, you need to create a new macOS compliance policy but you are unsure of which settings to configure.

You can use Copilot to quickly obtain the information that you need to:

1. learn which settings to configure,
2. determine the recommended values for the various settings, and,
3. ensure that there are no conflicts with existing policies.

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

Prompt	Expected outcome
Tell me about Intune setting "Stealth Mode"	<p>Go to Devices and select macOS. Then click on <i>Compliance</i> -> <i>Create Policy</i> -><i>Create</i>.</p> <p>After providing a policy name and description (optional), click "Next" to check the "<i>Compliance Settings</i>". Expanding "System Security" to see the setting "<i>Stealth Mode</i>" and click the Copilot button next to it:</p>  <p>A description of the setting is presented, as well as any relevant sources, supporting you in defining macOS compliance settings for your organization:</p>

	<p> Copilot (preview) X</p> <p>Tell me about Intune setting "Stealth Mode"</p> <p>The "Stealth Mode" setting for macOS in Intune is part of the SystemSecurity category under the ComplianceMac policy type. When enabled, Stealth Mode prevents the device from responding to probing requests, which can be made by malicious users. However, the device will still answer incoming requests for authorized applications. By default, this setting is not configured, meaning stealth mode is turned off [1].</p> <p>The setting is not required, and its primary purpose is to enhance the security of macOS devices by reducing their visibility to potential attackers [1].</p> <p>Sources:</p> <p>System security settings </p> <p>AI generated content may be incorrect. Check it for accuracy.  </p> <p>How could this setting affect users? </p> <p>Does Microsoft recommend any particular value for this setting? </p> <p>Generated by Microsoft Security Copilot  Learn more </p>
Has this setting been configured in any other policies?	Click on the book symbol in the bottom right of the window to see the suggested prompts in the guide to explore further:

The setting is not required, and its primary purpose is to enhance the security of managed devices against malicious attackers [1].

Sources:

- [Tell me about Intune setting "Stealth Mode"](#)
- [Has this setting been configured in any other policies?](#)
- [Does Microsoft recommend any particular value for this setting?](#)
- [How could this setting affect users?](#)
- [How could this setting affect security?](#)

AI generated

Does Microsoft recommend any particular value for this setting?

Generated by Microsoft Security Copilot [Learn more](#)

Next select the "Has this setting been configured in any other policies?" to avoid potential conflicts before deploying this new compliance policy:

	<p> Copilot (preview) X</p> <p>Has this setting been configured in any other policies?</p> <p>The "Stealth Mode" setting for macOS in Intune has been configured in the following policy:</p> <ul style="list-style-type: none"> • Policy Name: Alpine Ski House macOS Compliance - Integrity Protection • Policy ID: e6476270-0d1e-4ce9-9753-cfd745db7868 • Platform: macOS • Policy Type: Mac compliance policy • Last Modified: 2024-10-14T04:57:18Z • Is Assigned: False • Policy Link: Policy Link <p>Value of the given setting:</p> <ul style="list-style-type: none"> • Stealth Mode: Not configured <p>This policy is the only one in your account that includes the "Stealth Mode" setting for macOS. The setting is currently not configured in this policy.</p> <p>AI generated content may be incorrect. Check it for accuracy. [Copy] [Edit]</p> <hr/> <p style="text-align: right;">How could this setting affect users? Does Microsoft recommend any particular value for this setting? [More]</p> <p style="text-align: right; font-size: small;">Generated by Microsoft Security Copilot [More] Learn more [More]</p>
Does Microsoft recommend any particular value for this setting?	Next select the book symbol to view suggested prompts, and this time selects the prompt to learn what Microsoft's recommendations are for the setting in your policy:

	<p> Copilot (preview) X</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>Microsoft does not provide a specific recommended value for the "Stealth Mode" setting on macOS. The setting can be configured as follows:</p> <ul style="list-style-type: none"> • Not configured (default): This leaves stealth mode turned off. • Enable: This turns on stealth mode, preventing the device from responding to probing requests, which can be made by malicious users. However, the device will still answer incoming requests for authorized applications [1]. <p>The primary purpose of enabling stealth mode is to enhance the security of macOS devices by reducing their visibility to potential attackers [1].</p> <p>Sources:</p> <p>System security settings 🔗</p> <p>AI generated content may be incorrect. Check it for accuracy. 📄 🔍</p> </div> <hr/> <div style="text-align: center; margin-top: 10px;"> <p>How could this setting affect users? How could this setting affect security? 🔗</p> <p>Generated by Microsoft Security Copilot Learn more 🔗</p> </div>
How could this setting affect users?	To identify how this setting might affect user experience and compliance settings, you'll run this prompt to learn about the effects of the setting to users. You can then use this information to optimize the setting value according to your organization's use cases.

	 Copilot (preview) X <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>How could this setting affect users?</p> <p>Enabling the "Stealth Mode" setting on macOS can have the following effects on users:</p> <ol style="list-style-type: none"> 1. Enhanced Security: When stealth mode is enabled, the device will not respond to probing requests from unauthorized sources. This reduces the device's visibility to potential attackers, enhancing overall security [1]. 2. Authorized Applications: Despite being in stealth mode, the device will still respond to incoming requests for authorized applications. This ensures that necessary communications and operations for approved apps continue without interruption [1]. 3. User Experience: Users might not notice any significant changes in their day-to-day operations, as the primary impact of stealth mode is on how the device handles unauthorized probing requests. However, users may experience fewer unauthorized access attempts and potential security threats [1]. <p>Overall, enabling stealth mode can provide a more secure environment for macOS users by reducing the risk of unauthorized access while maintaining the functionality of authorized applications.</p> <p>Sources:</p> <p>System security settings </p> <p>AI generated content may be incorrect. Check it for accuracy.  </p> <hr/> <p>How could this setting affect security? Tell me about Intune setting "Stealth Mode" </p> <p>Generated by Microsoft Security Copilot  Learn more </p> </div>
How could this setting affect security?	Lastly, you need to work with the security team to ensure the configuration is up to the organization's standards, so you use 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.

The image shows a Microsoft Copilot (preview) interface. At the top, it says "Copilot (preview)" next to a colorful icon. In the center, there's a question "How could this setting affect security?". Below that is a large text box containing information about macOS Stealth Mode. The text explains that enabling Stealth Mode significantly enhances security by preventing the device from responding to probing requests from malicious users, reducing visibility to potential attackers. It notes that the device will still respond to authorized applications. A source link "System security settings" is provided. Below the main text, a message says "AI generated content may be incorrect. Check it for accuracy." with a document icon and a refresh icon. At the bottom, there are three buttons: "Tell me about Intune setting 'Stealth Mode'", "Has this setting been configured in any other policies?", and "Generated by Microsoft Security Copilot" with a "Learn more" link.

How could this setting affect security?

Enabling the "Stealth Mode" setting on macOS can significantly enhance security by preventing the device from responding to probing requests made by malicious users. This reduces the device's visibility to potential attackers, thereby lowering the risk of unauthorized access. However, the device will still respond to incoming requests for authorized applications, ensuring that necessary communications and operations continue without interruption [1].

Overall, enabling stealth mode can provide a more secure environment for macOS users by reducing the risk of unauthorized access while maintaining the functionality of authorized applications.

Sources:

[System security settings](#)

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

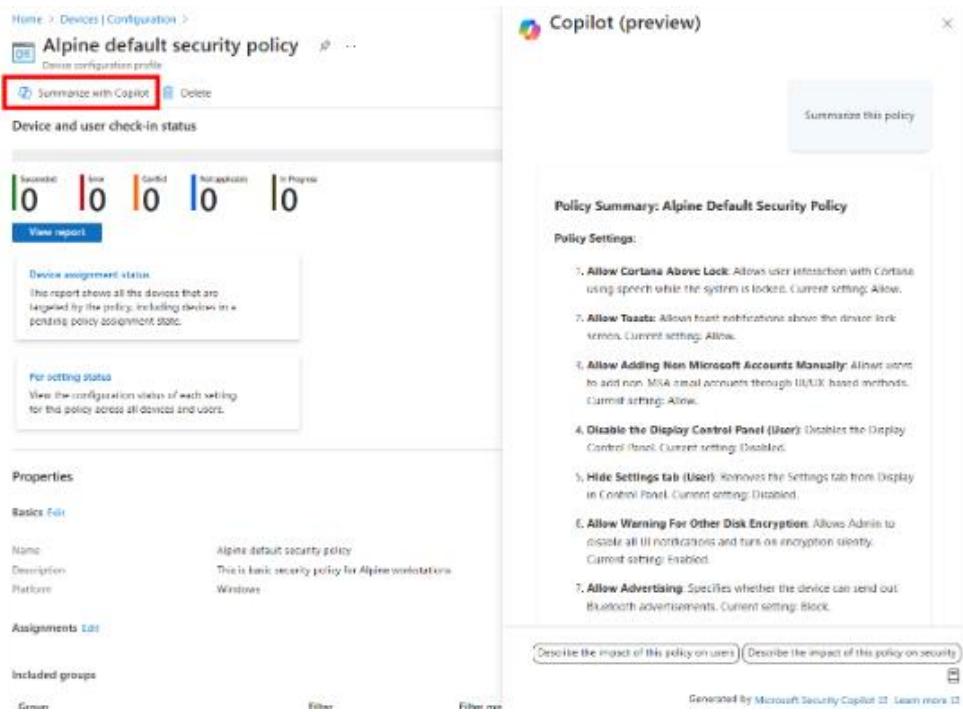
Tell me about Intune setting "Stealth Mode"

Has this setting been configured in any other policies?

Generated by Microsoft Security Copilot [Learn more](#)

Exercise 2: Policy Management: Summarization and Security Impact Assessment

You are a new IT admin that is tasked with reviewing and delivering a security policy for your environment encompassing BitLocker, ASR and more. You have inherited this task from another admin and was informed that some policies have already been created. You want to be able to summarize the existing policy and learn of its impact on users and security prior to creating new or editing existing policies.

Prompt	Expected outcome
Summarize this policy	<p>Navigate to the already existing policy by clicking on <i>Devices > Configuration</i> and then selecting the <i>Alpine default security policy</i>, and then click on the '<i>Summarize with Copilot</i>' 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>Policy Settings:</p> <ol style="list-style-type: none"> Allow Cortana Above Lock: Allows user interaction with Cortana using speech while the system is locked. Current setting: Allow. Allow Toasts: Allows toast notifications above the device lock screen. Current setting: Allow. Allow Adding New Microsoft Accounts Manually: Allows users to add non-MFA email accounts through UI/UX-based methods. Current setting: Allow. Disable the Display Control Panel (User): Disables the Display Control Panel. Current setting: Disabled. Hide Settings tab (User): Removes the Settings tab from Display in Control Panel. Current setting: Disabled. Allow Warning For Other Disk Encryption: Allows Admin to disable all UI notifications and turn on encryption silently. Current setting: Enabled. Allow Advertising: Specifies whether the device can send out Bluetooth advertisements. Current setting: Block. <p>Describe the impact of this policy on users Describe the impact of this policy on security</p>
Describe the impact of this policy on users	Click on the book icon to see the available prompts for this policy. Then select ' <i>Describe the impact of this policy on users</i> ' to understand what impact the settings and their values contained within this policy will have specifically on user experience when deployed:

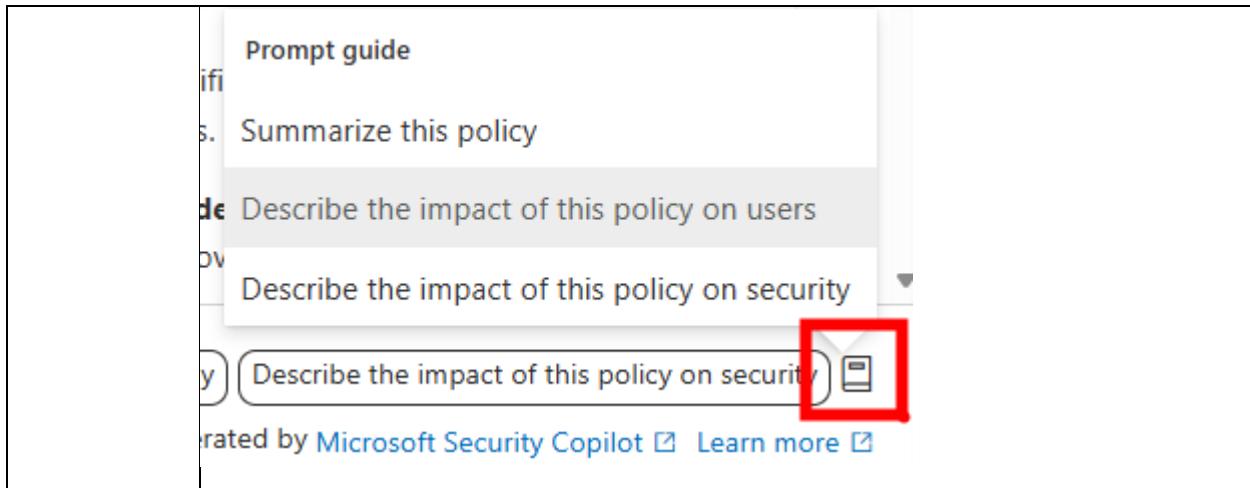
Prompt guide

Summarize this policy

Describe the impact of this policy on users

Describe the impact of this policy on security

Generated by Microsoft Security Copilot [Learn more](#)



	<p> Copilot (preview) X</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Describe the impact of this policy on users</p> </div> <h3>User Impact of Implementing the Alpine Default Security Policy</h3> <p>Implementing the Alpine Default Security Policy will have several impacts on users, primarily focusing on enhancing security while also affecting user experience and device functionality. Here are the key impacts:</p> <ol style="list-style-type: none"> 1. Cortana Interaction: Users will be able to interact with Cortana using speech even when the system is locked, which can improve productivity but may raise privacy concerns. 2. Toast Notifications: Allowing toast notifications above the lock screen ensures users receive important alerts and updates without unlocking their devices, enhancing convenience. 3. Non-Microsoft Accounts: Users can add non-Microsoft email accounts through UI/UX-based methods, providing flexibility in email management. 4. Display Control Panel: Disabling the Display Control Panel and hiding the Settings tab will restrict users from changing display settings, which can prevent misconfigurations but may be inconvenient for users needing to adjust their display. 5. Disk Encryption Warnings: Enabling silent encryption without warnings can enhance security but may lead to issues if third-party encryption is present, potentially rendering devices unusable. <p style="text-align: center;"> Summarize this policy Describe the impact of this policy on security  Generated by Microsoft Security Copilot Learn more  </p>
Describe the impact of this policy on security	Click on the book icon and this time select ' <i>Describe the impact of this policy on security</i> ' to understand what impact the settings and the values contained within this policy will have on the security of devices when deployed.



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 a significant impact on the security posture of the devices and users within the organization. Here are the key security impacts:

- 1. Allow Cortana Above Lock:** Allowing Cortana interaction above the lock screen can pose a security risk as it enables voice interactions with the device when it is locked. This could potentially be exploited to access sensitive information or perform unauthorized actions.
- 2. Allow Toasts:** Allowing toast notifications above the lock screen can expose sensitive information when the device is locked, which could be a security concern in shared or public environments.
- 3. Allow Adding Non Microsoft Accounts Manually:** Allowing users to add non-Microsoft email accounts can introduce security risks by potentially allowing less secure email accounts to be used on the device.
- 4. Disable the Display Control Panel (User):** Disabling the Display Control Panel prevents users from changing display settings, which can help maintain a consistent security configuration and prevent users from making potentially insecure changes.
- 5. Hide Settings tab (User):** Hiding the Settings tab from the

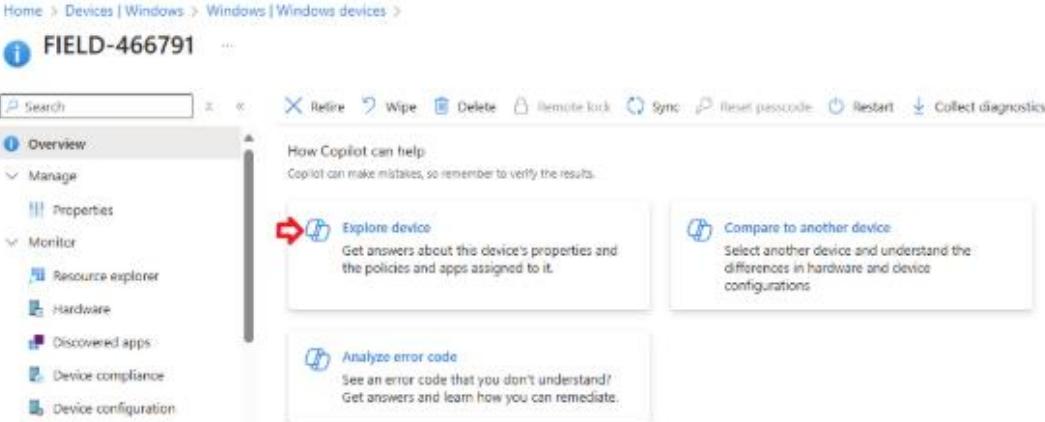
[Summarize this policy](#) [Describe the impact of this policy on users](#) 

Generated by Microsoft Security Copilot 

Exercise 3: Troubleshooting – Device summarization and Comparison

You are a helpdesk admin tasked with troubleshooting devices in Intune. You are facing a situation where a user is able to successfully elevate and install a particular app on one device, but not on another.

You suspect that Endpoint Privilege Manager (EPM) policies are missing from one device (FIELD-466791) but are applied successfully on another device (FIELD-694635). You need to quickly understand more about the devices and compare their policies to confirm your suspicions

Prompt	Expected outcome
Summarize this device	<p>Navigate to the device experiencing issues, Devices -> All Devices -> FIELD-466791 and select the '<i>Explore with Copilot</i>' button to see the available prompts and then selects '<i>Summarize this device</i>'.</p> <p>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.</p> <p>Please Note: You may be provided with an option to "<i>Explore device</i>" instead of the "<i>Explore with Copilot</i>" button as shown below:</p> 

The screenshot shows the Microsoft Intune Device Details page for a device named FIELD-466791. The left pane contains a navigation menu with sections like Overview, Manage, Monitor, Resource explorer, 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, Remediations (preview), and Device query. A red box highlights the "Explore with Copilot" button in the top right corner of the main content area. The right pane is titled "Copilot (preview)" and contains a message: "Ready to explore this device? Copilot can provide AI-generated insights to help you troubleshoot." Below this are several suggestions: "Summarize this device", "Analyze an error code", "Compare this device with another device", "Show apps on this device", "Show policies assigned to this device", and "Show group membership". At the bottom, it says "Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us." and "You can always use the prompt guide for suggestions by selecting this button".

	 <h2>Copilot (preview)</h2> <div style="text-align: right;">X</div> <div style="text-align: center; margin-top: 20px;"> Summarize this device </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"> <p>Device Information for c77b42f0-45c2-4e43-98e1-0602e6b9d990</p> <ul style="list-style-type: none"> • Intune Device ID: c77b42f0-45c2-4e43-98e1-0602e6b9d990 • Device Name: FIELD-466791 • Azure AD Device ID: 6246a2cc-6c10-4949-acde-7c1c14309506 • Azure AD Device Object ID: 9cc16d71-e845-4759-b072-cad9e644f528 <p>Device Compliance</p> <ul style="list-style-type: none"> • Compliance State: Compliant <p>Device Groups</p> <ul style="list-style-type: none"> • Number of Groups: 2 <ul style="list-style-type: none"> ◦ Group 1: All Autopilot Devices ◦ Group 2: All Autopilot Field Devices <p>User Information</p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;"> Show apps on this device Show policies assigned to this device  </div> <div style="text-align: center; margin-top: 5px;"> <small>Generated by Microsoft Security Copilot  Learn more </small> </div> </div>
Compare this device with another device	Compare the device in question with another device (FIELD-694635) that can successfully elevate the app. To assist with troubleshooting, ask Copilot to compare the device with the missing policies with the device that has the policies successfully applied.

To do so, click on the book icon and select 'Compare this device with another device'. Supply the name of the device (FIELD-694635) in *Device 2* field and select 'Configuration profiles' as the comparison type.

Copilot will compare policies applied on both devices and highlight any differences.

The screenshot shows the Microsoft Security Copilot (preview) interface. At the top, there's a button labeled "Compare this device with another device". Below it, a form asks "Select another device and what you want to compare". The "Device 2" field contains "FIELD-694635". The "Comparison type" dropdown is set to "Configuration profiles". A "Submit" button is at the bottom of the form. The main content area is titled "Comparison of Device Configuration Policies". It has a "Summary" section listing two devices:

- FIELD-466791** (Device ID: c77b42f0-45c2-4e43-9fe1-0602e6b9d990) has a total of 22 distinct device configuration policies, generating 38 status reports.
- FIELD-694635** (Device ID: 7fd6b1eb-45fd-4e49-a958-e45d943bc8cc) has a total of 24 distinct device configuration policies, generating 36 status reports.

Below this is a "Differences in Configuration Policies" section with two bullet points:

- FIELD-466791 has 0 different configuration policies.
- FIELD-694635 has 2 different configuration policies.

Policy Name	Policy Status	UPN
Intune EPM Settings	Succeeded	u2544@ash.alpineskithouse.co
Intune EPM Rules - PowerToys	Succeeded	u2544@ash.alpineskithouse.co

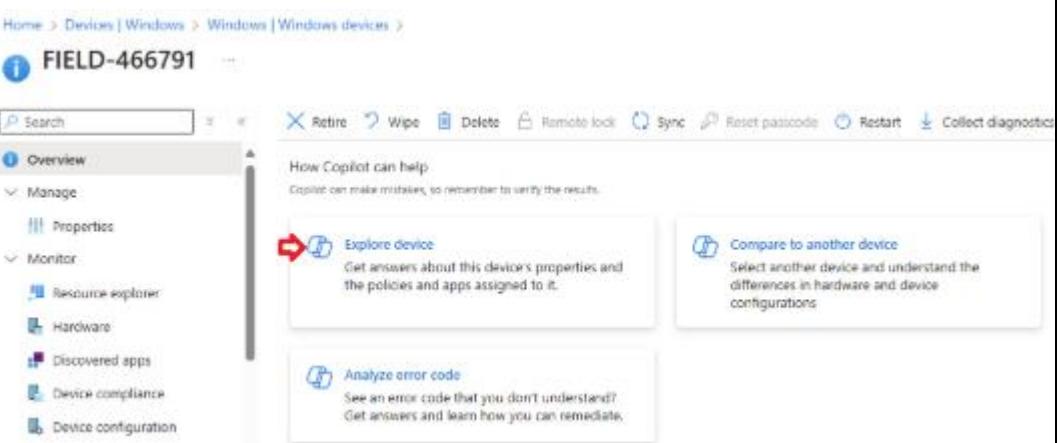
The text below the table states: "The device FIELD-466791 has no unique configuration policies, while FIELD-694635 has two unique configuration policies: "Intune EPM Settings" and "Intune EPM Rules - PowerToys", both of which have succeeded for the user u2544@ash.alpineskithouse.co."

At the bottom, there are "Sources:" links for "Microsoft Intune" and "Microsoft Intune". It also says "AI generated content may be incorrect. Check it for accuracy." with icons for a refresh and a checkmark. Navigation buttons at the bottom include "Summarize this device", "Compare this device with another device", and links for "Generated by Microsoft Security Copilot" and "Learn more".

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

Exercise 4: Troubleshooting – Error Codes

Whilst troubleshooting, you came across some error codes on the device (FIELD-466791) that you do not know the meaning of and decide to ask Copilot what they correlate to.

Prompt	Expected outcome
Analyze an error code (0x800B0109)	<p>You found an error code whilst troubleshooting the device, but you are not sure what it correlates to and decide to ask Copilot.</p> <p>Navigate to the device in question and click on the '<i>Explore with Copilot</i>' button and select '<i>Analyze an error code</i>'. Enter error code (0x800B0109) and click '<i>Submit</i>'.</p> <p>Copilot will provide an explanation of the error code to assist you with troubleshooting and resolution.</p> <p>Please Note: You may be provided with an option to "<i>Explore device</i>" instead of the "<i>Explore with Copilot</i>" button as shown below:</p> 

The screenshot shows two side-by-side interfaces. On the left is the Microsoft Intune Device Overview page for a device named 'FIELD-466791'. The top navigation bar includes 'Home > Devices | Windows > Windows | Windows devices > FIELD-466791'. Below the navigation is a search bar and a red box highlights the 'Explore with Copilot' button. A sidebar on the left lists various management and monitoring options. The main content area displays device details such as 'Device name: FIELD-466791', 'Management name: u2546_Windows_1/10/2025_1158 AM', 'Ownership: Corporate', 'Serial number: 0E55-423E-5452-6471-0B09-2545-19', 'Phone number: ***', and 'Device manufacturer: Microsoft Corporation'. Below this is a table titled 'Device actions status' with columns 'Action' and 'Status', showing 'No data'. On the right is the 'Copilot (preview)' interface, which is a card-based tool for troubleshooting. It features a heading 'Ready to explore this device? Copilot can provide AI-generated insights to help you troubleshoot.', a 'Summarize this device' section, and a prominent red box around the 'Analyze an error code' button. Other buttons include '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. In help improve the experience, please share your feedback with us.' and 'You can always use the prompt guide for suggestions by selecting this button'. At the bottom of the Copilot card is a form with a placeholder 'Enter an error code to analyze.', a red box around the 'Error code' input field containing '0x0000109', and a 'Submit' button. Below the Copilot card are links 'View prompt', 'Generated by Microsoft Security Copilot', and 'Learn more'.

Copilot (preview)

Enter an error code to analyze.

Error code * ⓘ

0x800B0109

Submit

The error code 0x800B0109 indicates a certificate error. This error 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 due to a certificate issue. The error message logged in the SoftwareDistribution.log file is: "The given certificate chain has not Microsoft Root CA signed root (800B0109)" [1].

To resolve this issue, you need to ensure that the WSUS application on the server is SHA2-compliant. You can do this by downloading and installing the Update for Windows Server 2008 R2 for x64-based Systems (KB4484071) released on November 12, 2019. No reboot is required after installing this update [1].

If you encounter this error in a different context, such as when clients try to access the CMG cloud service, it may be due to a mismatch between the default FQDN and the actual FQDN. Updating to Configuration Manager current branch version 1902 can resolve this issue [2].

In summary, the error code 0x800B0109 is related to certificate issues, and the resolution steps depend on the specific context in which the error occurs. The provided documents offer detailed guidance on how to address this error in different scenarios.

Sources:

[WSUS doesn't sync with Microsoft on Windows Server 2008 R2 servers because of a certificate error](#) ⓘ

[Cause](#) ⓘ

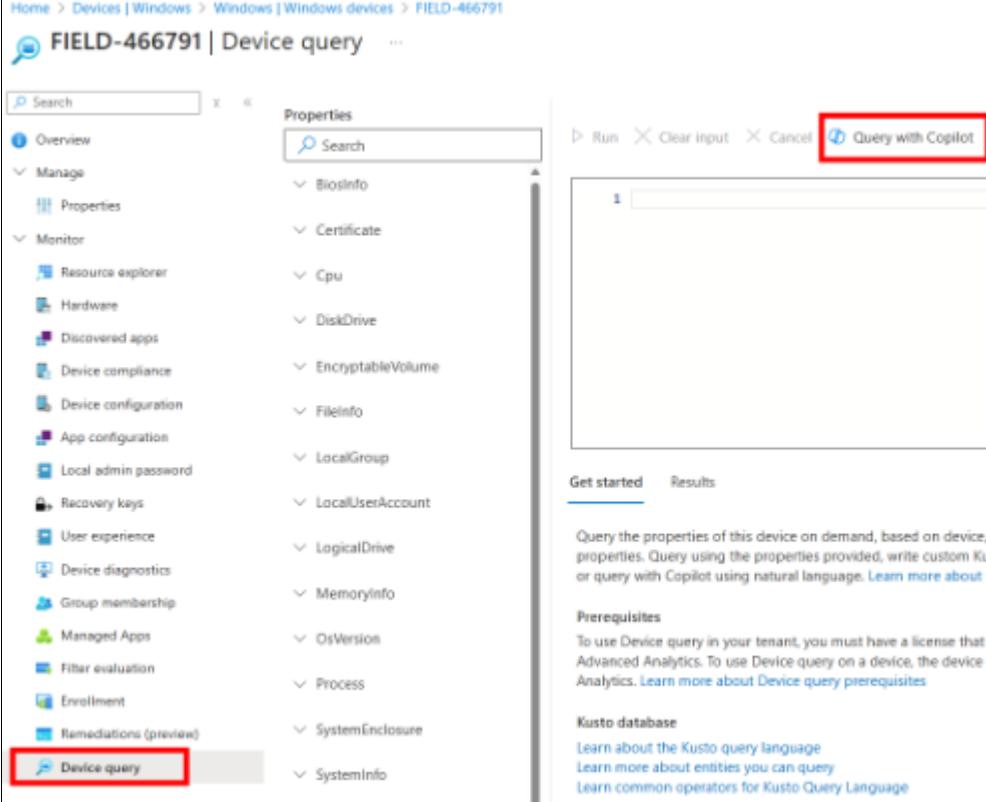
AI generated content may be incorrect. Check it for accuracy. ⓘ ⓘ

Analyze an error code ⓘ

Generated by Microsoft Security Copilot ⓘ Learn more ⓘ

Exercise 5: Copilot into Single Device Query

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

Prompt	Expected outcome
What are the top 10 processes using the most memory on this device?	You start by investigating what processes might be causing this, so you select the device (FIELD-466791) in the Microsoft Intune admin center and go to the 'Device query' tab then click on 'Query with Copilot' to ask Copilot to write the appropriate KQL query for your prompt. 

Click 'Add and Run' to see the results of the query.



Copilot (preview)

X

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 | top 10 by WorkingSetSizeBytes desc | project  
ProcessId, ProcessName, WorkingSetSizeBytes
```

Add to editor

Add and run

How was this query generated?

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

View prompts

What would you like to know about this device?

Generated by Microsoft Security Copilot

The query is automatically added to the editor and executed.

	<p>Run ▶ Clear input × Cancel ? Query with Copilot</p> <pre>1 // Generated by Copilot 2 Process top 10 by WorkingSetSizeBytes desc project Pi</pre> <p>Get started Results</p> <p>Columns Device Actions 10 items</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ProcessId</th><th>ProcessName</th><th>WorkingSetSizeBytes</th></tr> </thead> <tbody> <tr><td>4312</td><td>MsMpEng.exe</td><td>269946880</td></tr> <tr><td>4240</td><td>MsSense.exe</td><td>133361664</td></tr> <tr><td>5796</td><td>Microsoft.Management... ...ment</td><td>94330880</td></tr> <tr><td>2196</td><td>LogonUI.exe</td><td>87150592</td></tr> <tr><td>4168</td><td>svchost.exe</td><td>64430080</td></tr> <tr><td>6944</td><td>SenseNdr.exe</td><td>62767104</td></tr> <tr><td>2180</td><td>dwm.exe</td><td>56291328</td></tr> <tr><td>2612</td><td>svchost.exe</td><td>53014528</td></tr> <tr><td>4304</td><td>OfficeClickToRun.exe</td><td>46477312</td></tr> <tr><td>5240</td><td>SenseCE.exe</td><td>42758144</td></tr> </tbody> </table> <p>You can use the scroll bars to see the additional columns and rows returned.</p>	ProcessId	ProcessName	WorkingSetSizeBytes	4312	MsMpEng.exe	269946880	4240	MsSense.exe	133361664	5796	Microsoft.Management... ...ment	94330880	2196	LogonUI.exe	87150592	4168	svchost.exe	64430080	6944	SenseNdr.exe	62767104	2180	dwm.exe	56291328	2612	svchost.exe	53014528	4304	OfficeClickToRun.exe	46477312	5240	SenseCE.exe	42758144
ProcessId	ProcessName	WorkingSetSizeBytes																																
4312	MsMpEng.exe	269946880																																
4240	MsSense.exe	133361664																																
5796	Microsoft.Management... ...ment	94330880																																
2196	LogonUI.exe	87150592																																
4168	svchost.exe	64430080																																
6944	SenseNdr.exe	62767104																																
2180	dwm.exe	56291328																																
2612	svchost.exe	53014528																																
4304	OfficeClickToRun.exe	46477312																																
5240	SenseCE.exe	42758144																																
Show me the top 20 running processes on this device and exclude wmiclipse	<p>You also want 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.</p> <p>You also want to ensure that the process for WMI Provider Host is excluded. Click on the 'Query with Copilot' button and in the query box, enter the prompt in Copilot "Show me the top 20 running processes on this device and exclude wmiclipse" to write the KQL query.</p> <p>Once Copilot has returned the KQL query, select 'Add and run' to automatically execute the query.</p>																																	

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
| where ProcessName != 'wmicprvse'
| top 20 by ElapsedTimeMilliseconds desc
| project ProcessId, ProcessName, ElapsedTimeMilliseconds
```

[Add to editor](#) [Add and run](#)

How was this query generated?

AI generated content may be incorrect. Check it for accuracy. [🔗](#) [ⓘ](#)

Run Clear input Cancel [Query with Copilot](#)

```
1 // Generated by Copilot
2 //Process | top 10 by WorkingSetSizeBytes desc | project
3
4 // Generated by Copilot
5 Process
6 | where ProcessName != 'wmicprvse'
7 | top 20 by ElapsedTimeMilliseconds desc
8 | project ProcessId, ProcessName, ElapsedTimeMilliseconds
```

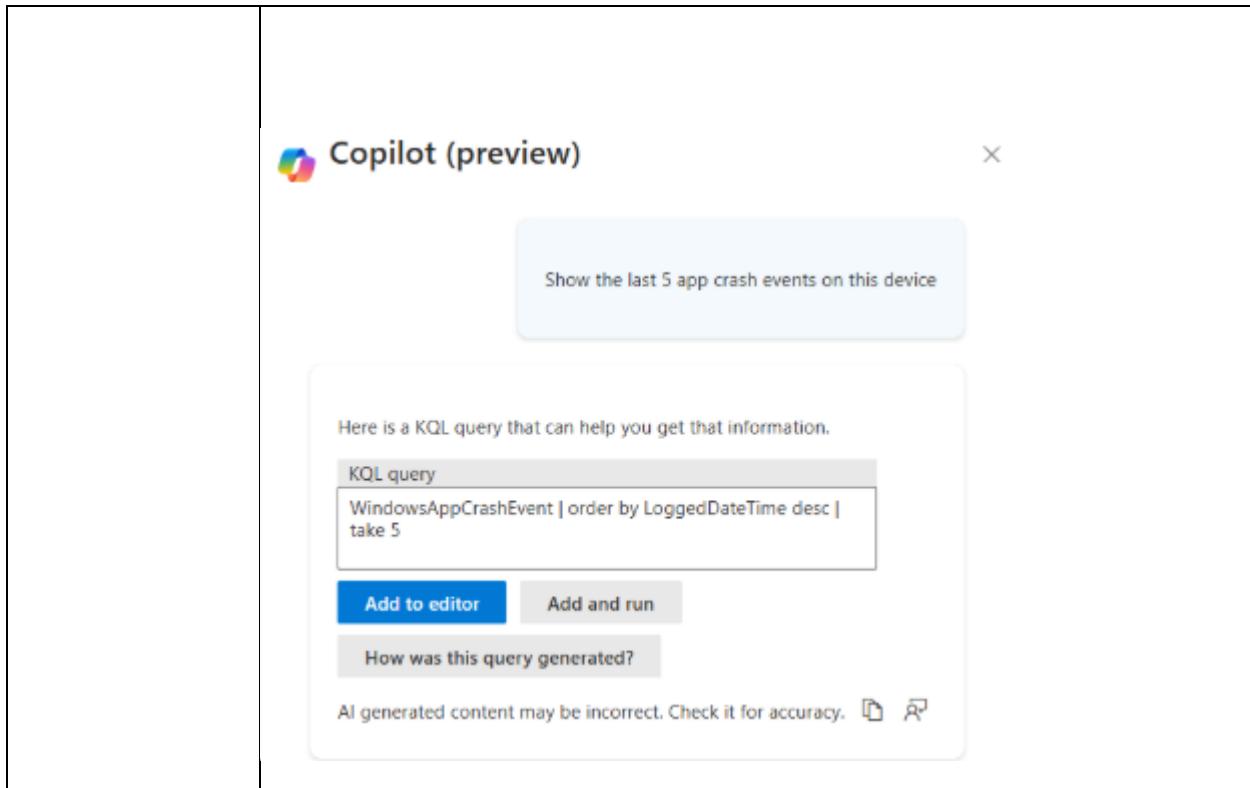
Get started Results

Columns Device Actions 20 items

ProcessId	ProcessName	ElapsedTimeMilliseconds
180	Registry	626542
140	Secure System	626520
732	smss.exe	624287

Show the last 5 app crash events on this device

You see a number of processes associated with apps and want to understand if the slowness might be caused by application crashes. Use the 'Query with Copilot' to ask for a query that can show you the last 5 app crash events on that device.



The screenshot shows the Security Copilot interface. At the top, there's a toolbar with 'Run' (blue triangle), 'Clear input' (cross), 'Cancel' (cross), and 'Query with Copilot' (blue icon). Below the toolbar is a code editor window containing the following PowerShell-like query:

```

8 //Process | where ProcessName != 'wmiprvse' | to
9
10 // Generated by Copilot
11 WindowsAppCrashEvent | order by LoggedDateTime de

```

Below the code editor is a table titled 'Results'. It has columns: ReportId, AppPath,AppName, AppVersion, and Log. The data in the table is as follows:

ReportId	AppPath	AppName	AppVersion	Log
5716	C:\Windows\uu...	MoUsoCoreWo...	1308.2407.1504...	202
5579	C:\Windows\uu...	MoUsoCoreWo...	1308.2407.1504...	202
5462	C:\Windows\uu...	MoUsoCoreWo...	1308.2407.1504...	202

At the bottom of the interface, there is a note: **Please note:** It is possible that this query may not return any results based on the availability of app crash events.

Exercise 6: Intune Standalone

In this exercise we'll be using the standalone portal to investigate a device that is potentially suspicious. This device is Intune managed and is currently in use.

1. Login to Security Copilot [<https://securitycopilot.microsoft.com>] and sign in with your credentials.
2. Start a new session and enter the prompts below:

Prompt	Expected outcome
Show me the devices for	Ask Security Copilot to show all the devices for the specified user

<p>the user u2544</p>	<p>Show me the devices for the user u2544</p> <p>> 3 steps completed 14 seconds</p> <p>Jan 10, 4:19 PM</p> <h3>User Information</h3> <ul style="list-style-type: none"> User ID: e22d6804-aff5-4ed2-a2f1-0c1fa25ed17f Display Name: u2544 Usage Location: FR User Principal Name: u2544@ash.alpineskihouse.co Created Date: 2024-09-17T22:48:17Z <h3>User Groups</h3> <ul style="list-style-type: none"> This user is a member of 16 user groups. For more details, visit User Groups. <h3>Devices</h3> <p>This user has a total of 4 Intune Managed devices.</p> <table border="1" data-bbox="401 973 1274 1402"> <thead> <tr> <th data-bbox="425 1072 551 1100">Device Name</th><th data-bbox="703 1072 850 1100">Intune Device ID</th><th data-bbox="980 1072 1095 1100">Enrolled Date</th></tr> </thead> <tbody> <tr> <td data-bbox="425 1127 551 1176">FIELD-689193</td><td data-bbox="703 1127 931 1176">e0af4dc0-6ea2-4ac6-ad85-beb6d6415eec</td><td data-bbox="980 1127 1209 1176">2025-01-10T01:28:23+00:00</td></tr> <tr> <td data-bbox="425 1199 551 1227">FIELD-466791</td><td data-bbox="703 1199 931 1227">c77b42f0-45c2-4e43-98e1-0602e6b9d990</td><td data-bbox="980 1199 1209 1227">2025-01-10T01:28:23+00:00</td></tr> <tr> <td data-bbox="425 1271 551 1298">FIELD-694635</td><td data-bbox="703 1271 931 1320">7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc</td><td data-bbox="980 1271 1209 1298">2024-10-11T01:34:37+00:00</td></tr> <tr> <td data-bbox="425 1343 551 1370">FIELD-340181</td><td data-bbox="703 1343 931 1391">2feb9045-856a-4625-91a4-26cd56b08ab2</td><td data-bbox="980 1343 1209 1370">2024-10-11T01:31:34+00:00</td></tr> </tbody> </table> <p>To verify Intune managed devices in the Intune console, you can navigate to the Troubleshooting + support page, choose Troubleshoot, and search using User Principal Name or Display Name: u2544@ash.alpineskihouse.co.</p>	Device Name	Intune Device ID	Enrolled Date	FIELD-689193	e0af4dc0-6ea2-4ac6-ad85-beb6d6415eec	2025-01-10T01:28:23+00:00	FIELD-466791	c77b42f0-45c2-4e43-98e1-0602e6b9d990	2025-01-10T01:28:23+00:00	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-689193	e0af4dc0-6ea2-4ac6-ad85-beb6d6415eec	2025-01-10T01:28:23+00:00														
FIELD-466791	c77b42f0-45c2-4e43-98e1-0602e6b9d990	2025-01-10T01:28:23+00:00														
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														
<p>Show me a summary of the Intune device field-694635</p>	<p>You then ask about the potentially faulty device and get extensive information about its current configuration state.</p>															

Show me a summary of the Intune device field-694635

> 3 steps completed 13 seconds

Jan 10, 10:12 AM

Device Summary for FIELD-694635

- **Intune Device ID:** 7fd6b1eb-451d-4e49-a9f8-e45d9438c8cc
- **Device Name:** FIELD-694635
- **Azure AD Device ID:** 2e52b14a-4eb9-4bc0-8129-5860f60c3a4b
- **Operating System:** Windows 10.0.26100.2605
- **Compliance State:** Compliant
- **Management State:** Managed
- **Owner Type:** Company
- **Device Type:** WindowsRT
- **Enrolled Date:** 2024-10-11T01:34:37.390303Z
- **Last Sync Date:** 2025-01-10T13:10:46.821528Z
- **User Principal Name:** u2544@ash.alpineskihouse.co
- **Model:** Virtual Machine
- **Manufacturer:** Microsoft Corporation
- **Serial Number:** 3311-9857-3961-4236-2773-5354-36
- **Ethernet MAC Address:** 00155D01040D
- **Total Storage Space:** 63.44 GB
- **Free Storage Space:** 26.32 GB
- **Primary User:** u2544
- **Last Logon Time:** 2025-01-10T12:52:35.814153Z

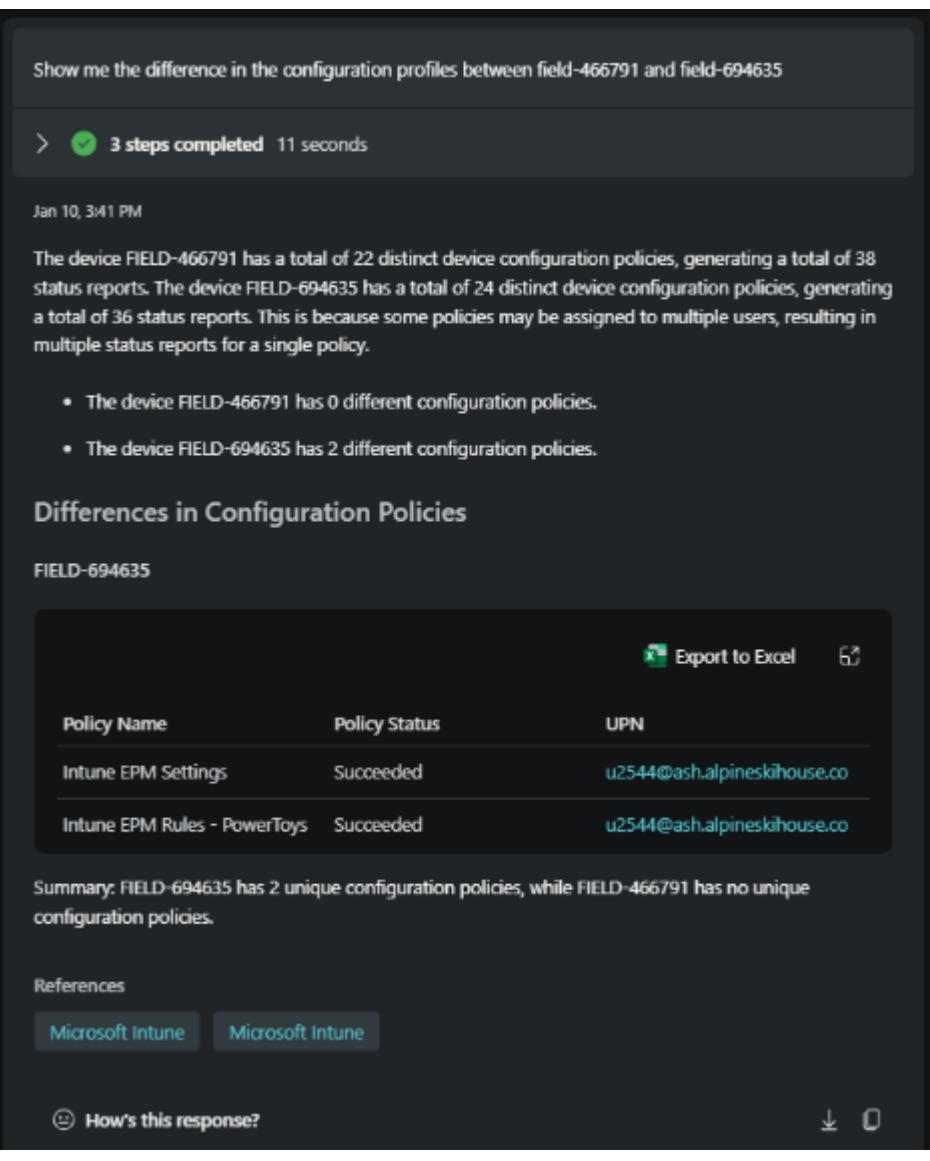
Device Group Membership

- **Total Groups:** 3
 - Intune EPM Demo Devices
 - All Autopilot Devices
 - All Autopilot Field Devices

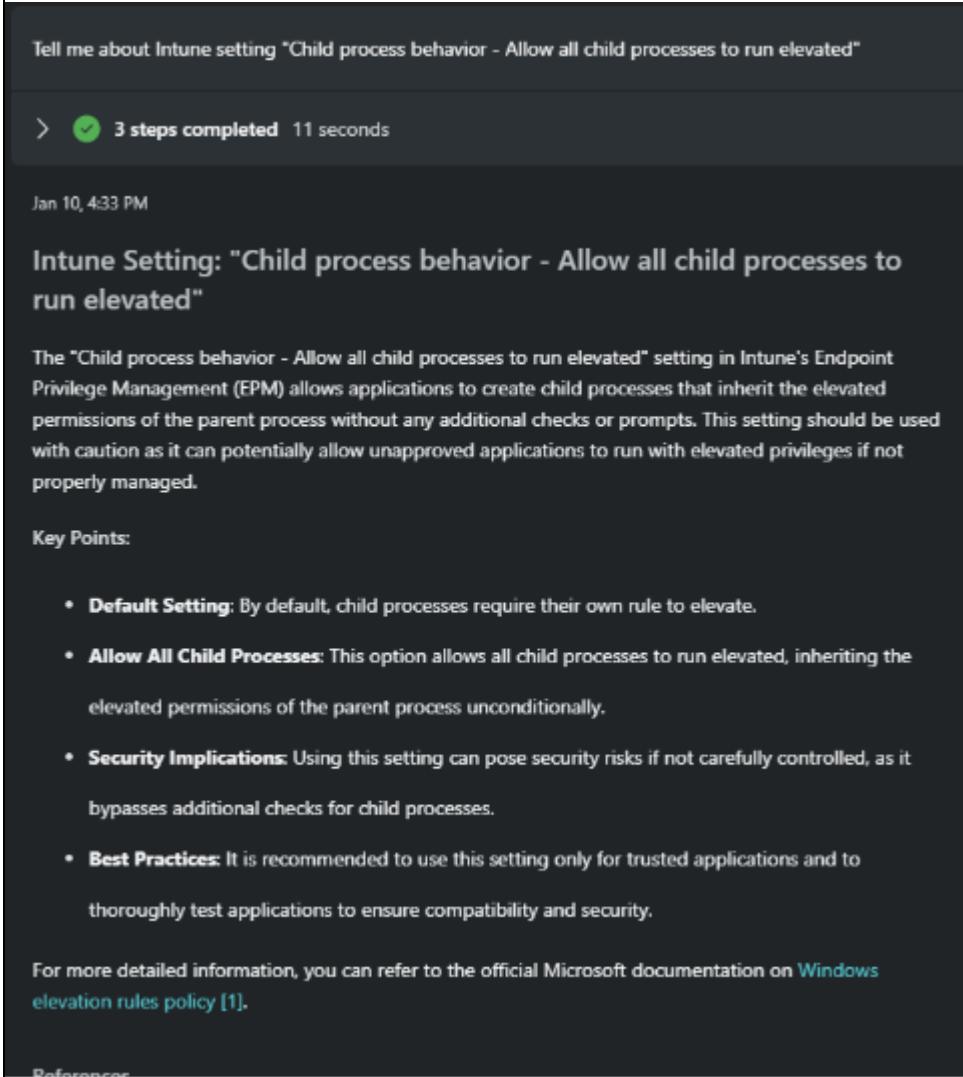
No noncompliance reasons were found for this device.

References

[Microsoft Intune](#) [Microsoft Intune](#)

<p>Show me the difference in the configuration profiles between field-466791 and field-694635</p>	<p>You ask Security Copilot if there's any difference in configuration between the potentially compromised device and a known working and uncompromised device, so that you can determine if there is a missing setting causing an issue.</p>  <p>The screenshot shows the Microsoft Copilot interface. At the top, a query is displayed: "Show me the difference in the configuration profiles between field-466791 and field-694635". Below this, a progress bar indicates "3 steps completed 11 seconds". The date "Jan 10, 3:41 PM" is shown. The main content area displays a summary of configuration policies for both devices:</p> <table border="1"> <thead> <tr> <th>Policy Name</th> <th>Policy Status</th> <th>UPN</th> </tr> </thead> <tbody> <tr> <td>Intune EPM Settings</td> <td>Succeeded</td> <td>u2544@ash.alpineskihouse.co</td> </tr> <tr> <td>Intune EPM Rules - PowerToys</td> <td>Succeeded</td> <td>u2544@ash.alpineskihouse.co</td> </tr> </tbody> </table> <p>A summary message states: "Summary: FIELD-694635 has 2 unique configuration policies, while FIELD-466791 has no unique configuration policies." Below this, a "References" section lists "Microsoft Intune" twice. At the bottom, there is a "How's this response?" button with a thumbs-up/thumbs-down icon.</p>	Policy Name	Policy Status	UPN	Intune EPM Settings	Succeeded	u2544@ash.alpineskihouse.co	Intune EPM Rules - PowerToys	Succeeded	u2544@ash.alpineskihouse.co
Policy Name	Policy Status	UPN								
Intune EPM Settings	Succeeded	u2544@ash.alpineskihouse.co								
Intune EPM Rules - PowerToys	Succeeded	u2544@ash.alpineskihouse.co								
<p>Show me the summary for the policy Intune EPM</p>	<p>You suspect the issue might be related to a specific policy – the Endpoint Privileged Protection policy – so you ask Copilot to summarize it, so you can quickly review it.</p>									

Rules - PowerToys	<p>Show me the summary for the policy Intune EPM Rules - PowerToys</p> <p>> 3 steps completed 12 seconds</p> <p>Jan 10, 4:33 PM</p> <h3>Policy Summary: Intune EPM Rules - PowerToys</h3> <p>Policy Name</p> <ul style="list-style-type: none"> Intune EPM Rules - PowerToys <p>Settings Details</p> <ol style="list-style-type: none"> Elevation Rule Name - Applies to: All device users Elevation Rule Name - File hash: ECBEEED67EFA864E558403F719B7FFD6F0192F77C36579B2FF9C2A086DD305752 <ul style="list-style-type: none"> 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 <p>Assignment Scope</p> <ul style="list-style-type: none"> Included Groups: <ul style="list-style-type: none"> Group Name: Intune EPM Demo Devices Member Count: 1 Device Count: 1 User Count: 0 <p>Summary</p> <p>The "Intune EPM Rules - PowerToys" policy is configured to apply to all device users and is designed to elevate the PowerToysSetup-0.68.1-x64.exe file. The policy includes specific settings such as allowing all child processes to run elevated and requiring user confirmation for elevation. The policy is assigned to the "Intune EPM Demo Devices" group, which includes one device and no users.</p> <p>References</p> <p>Microsoft Intune</p>
Tell me about Intune setting "Child process behavior - Allow all child	From the previous policy summary, you suspect the issue might have originated from a specific setting, and that ' <i>Child process behavior - Allow all child processes to run elevated</i> ', that might not be configured correctly.

processes to run elevated"	<p>Ask Copilot to provide more information about this setting, so you can consider changing it.</p>  <p>The image shows a screenshot of a Copilot interface. At the top, there's a text input field with the placeholder "Tell me about Intune setting 'Child process behavior - Allow all child processes to run elevated'". Below the input field, there's a progress bar indicating "3 steps completed" in 11 seconds. The timestamp "Jan 10, 4:33 PM" is shown below the progress bar. The main content area is titled "Intune Setting: 'Child process behavior - Allow all child processes to run elevated'" and contains a detailed explanation of the setting. It states: "The 'Child process behavior - Allow all child processes to run elevated' setting in Intune's Endpoint Privilege Management (EPM) allows applications to create child processes that inherit the elevated permissions of the parent process without any additional checks or prompts. This setting should be used with caution as it can potentially allow unapproved applications to run with elevated privileges if not properly managed." Below this, a section titled "Key Points:" lists several bullet points: <ul style="list-style-type: none"> • Default Setting: By default, child processes require their own rule to elevate. • Allow All Child Processes: This option allows all child processes to run elevated, inheriting the elevated permissions of the parent process unconditionally. • Security Implications: Using this setting can pose security risks if not carefully controlled, as it bypasses additional checks for child processes. • Best Practices: It is recommended to use this setting only for trusted applications and to thoroughly test applications to ensure compatibility and security. <p>For more detailed information, you can refer to the official Microsoft documentation on Windows elevation rules policy [1].</p> <p><small>References</small></p> </p>
What are the threats associated with this user's devices?	<p>Lastly, ask Copilot if there are any threats associated with this user's devices, to ensure the environment remains safe.</p>

The screenshot shows the Microsoft Security Copilot interface. At the top, a question is asked: "What are the threats associated with this user's devices?". Below this, a list of completed steps is shown:

- 3 steps completed 19 seconds
 - Chose Natural language to KQL for Microsoft Defender XDR 6 seconds
 - Processed your request 9 seconds
 - Prepared your response 3 seconds

The timestamp Jan 10, 4:34 PM is displayed. The main content area is titled "Threats Associated with User's Devices". It states that the following KQL query was used:

```
1 let deviceNames = dynamic(["FIELD-689193", "FIELD-466201", "FIELD-694635", "FIELD-340101"]);  
2 IntuneDevices  
3 | where DeviceName in (deviceNames)  
4 | join kind=inner (AlertEvidence) on DeviceId  
5 | project Timestamp, AlertId, DeviceId, DeviceName, ThreatFamily, RemoteUrl, SHA256, AccountName, AccountUpn
```

Product Name: Defender
Total Row Count: 0
Displayed Row Count: 0
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](#)

Activity 6: Standalone and Extensibility

In this activity we will run built-in promptbook, create a promptbook and create a custom plugin from Security Copilot standalone

Estimated time to complete this activity

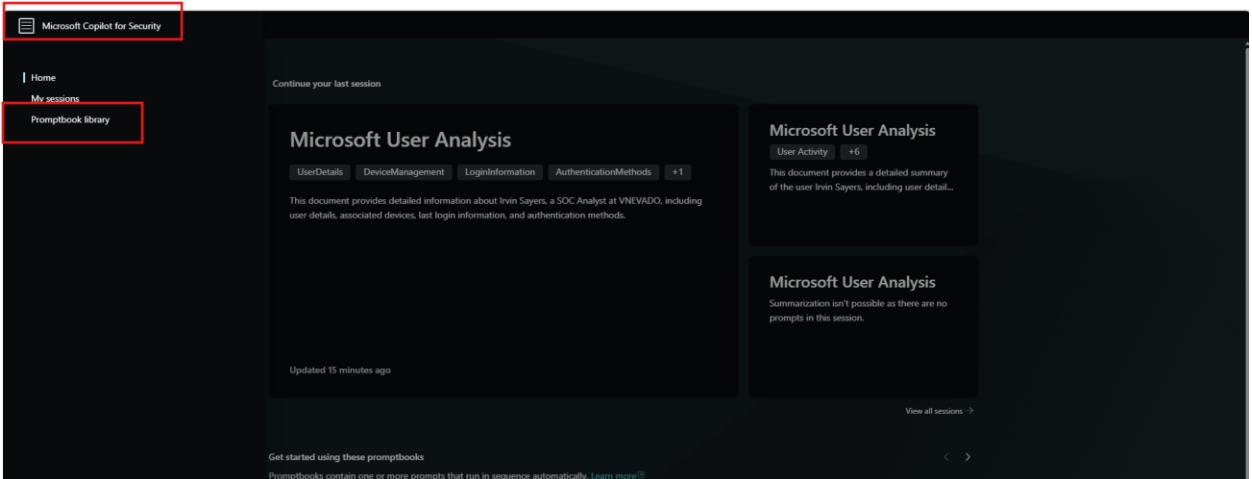
30 minutes

Exercise 1: Running built-in Promptbook

This exercise demonstrates how to run built-in promptbooks

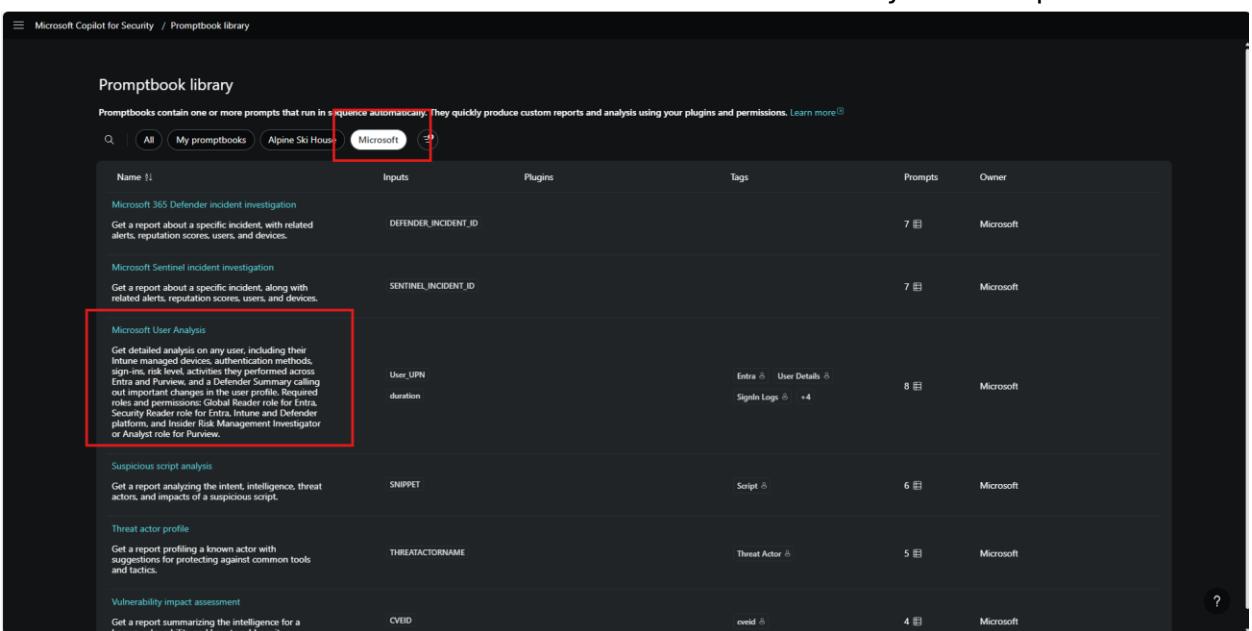
1. Login to <https://securitycopilot.microsoft.com/>

2. Select the  home menu in the left corner
3. Navigate to Promptbook library



The screenshot shows the Microsoft Copilot for Security interface. The left sidebar has a 'Promptbook library' option highlighted with a red box. The main content area displays a 'Microsoft User Analysis' promptbook. It includes a summary section, a detailed view of user activity, and a note that summarization is not possible because there are no prompts in the session. At the bottom, there's a link to 'View all sessions'.

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



The screenshot shows the 'Promptbook library' page with the 'Microsoft' tab selected. The 'Microsoft User Analysis' promptbook is highlighted with a red box. The table lists several other promptbooks, each with a brief description, inputs, plugins, tags, prompts, and owner information. The 'Microsoft' promptbook is owned by Microsoft and has 8 prompts.

Name	Inputs	Plugins	Tags	Prompts	Owner
Microsoft 365 Defender incident investigation	DEFENDER INCIDENT ID			7	Microsoft
Microsoft Sentinel incident investigation	SENTINEL INCIDENT ID			7	Microsoft
Microsoft User Analysis	User UPN duration	Entra User Details Signin Logs	8 +4	8	Microsoft
Suspicious script analysis	SNIPPET	Script	8	6	Microsoft
Threat actor profile	THREATACTORNAME	Threat Actor	8	5	Microsoft
Vulnerability impact assessment	CVEID	cveid	8	4	Microsoft

5. Click on “Start a new Session”

Promptbook library

Microsoft User Analysis

Created by Microsoft • 8 prompts

Tags: Entra, User Details, Signin Logs, Azure AD, Purview, Intune, Defender

Name: Microsoft

Inputs: User_UPN, duration

Prompts:

- 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>

Prompts	Owner
7	Microsoft
8	Microsoft
6	Microsoft
5	Microsoft
4	Microsoft

6. Field the details with “irvins@vnevado.alpineskihouse.co” and 14 days respectively

Submit

Microsoft User Analysis

Get 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 platforms, and Insider Risk Management Investigator or Analyst role for Purview.

User_UPN: irvins@vnevado.alpineskihouse.co

duration: 14 days

Prompts (8)

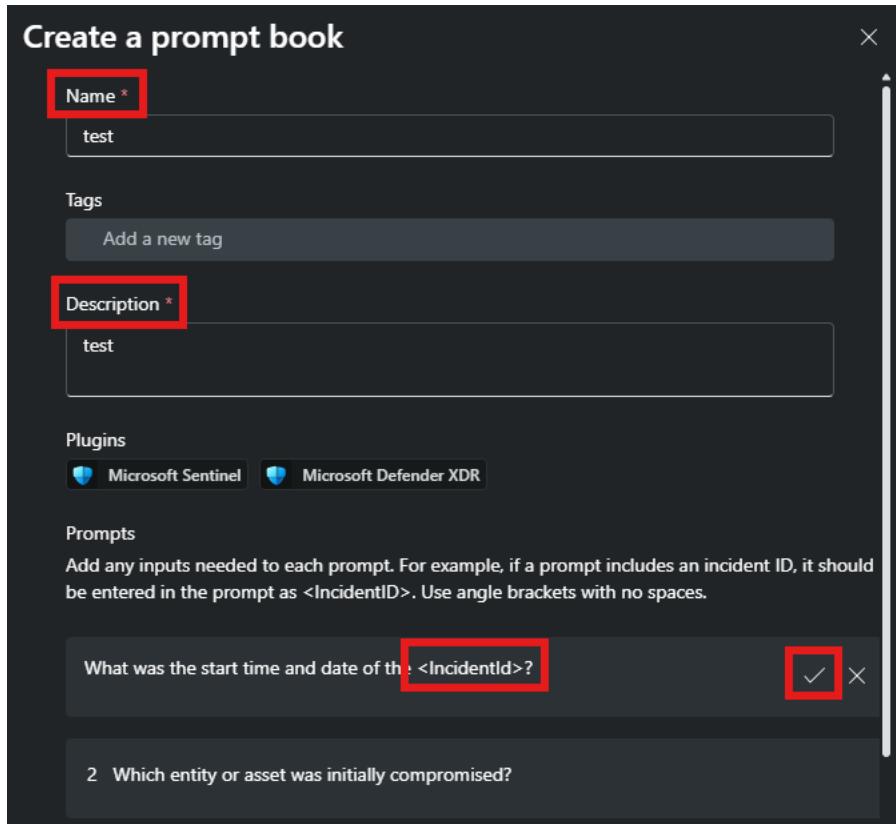
- 1 Tell me more about <User_UPN>?
- 2 What devices are associated with the above user?
- 3 Show me the last login for the above user during the last <duration>.
- 4 What authentication methods are set up for the above user?
- 5 Did the above user have any failed sign-ins during the last <duration>? 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>

7. Go through the results

Exercise 2: Create a Promptbook

This exercise demonstrates how to create a promptbook. In this scenario, we will create a promptbook from previously ran prompts in the Microsoft Defender XDR standalone [exercise 7](#)

1. Login to <https://securitycopilot.microsoft.com/>
2. Select the  home menu in the left corner and navigate to My Session
3. Click and open the session that was ran for Defender XDR standalone exercise 7
The name of the session should be 'Give me a summary of Defender incident 4078'
4. On the session, click on  to create a promptbook
5. Provide a name, description and for your first prompt change the Incident ID to a input by replacing it with <IncidentID> (use angle brackets) and click the check mark to save the updates



6. Click Create to save the promptbook
7. The newly created promptbook will be available in Promptbook library and can be run for any Incident by entering the Incident ID number

Exercise 3: Custom Plugin (Walkthrough only)

This exercise demonstrates how to create a KQL plugin for Copilot for Security Custom Plugin using the example of a KQL query to derive our Sentinel detailed costs. This includes explanations of Sentinel tables, detailed cost summaries, and cost-saving recommendations. This added context helps users better understand their Sentinel costs and optimize their security operations.

Configure and review the KQL Custom Plugin

1. Download [KQL-SentinelCost-Alpine-Ski.yaml](https://github.com/Azure/Security-Copilot Plugins/Community Based Plugins/Microsoft Sentinel Custom Plugin Scenarios/Sentinel Cost Query Plugin) to an accessible location.
[<https://github.com/Azure/Security-Copilot Plugins/Community Based Plugins/Microsoft Sentinel Custom Plugin Scenarios/Sentinel Cost Query Plugin>]
2. Open the yaml file in your favorite editor and review the settings. The file needs to be updated with Tenant Id, Subscription Id and workspace Id of the Sentinel instance

3. Click on the Source icon, located next to the prompt bar



4. Scroll down to Custom -> click Add plugin -> Select Security Copilot Plugin and upload the yaml file -> Click Add create the custom plugin

5. In the prompt bar, enter **Can you provide a detailed summary of the total of my Sentinel Costs of the past 90 days?**

6. Let's iterate and add more context, run the prompt **Provide a detailed summary of the total of my Sentinel Costs of the past 90 days. Outline for all tables what it is used for within Sentinel and the security value it provides, format as a table. Also total up all the cost to give me an average of monthly costs. Also be sure to give any costs savings recommendations based on my data ingestion.**

7. Lastly ask for recommendations, **How do my current data retention policies impact the costs of the largest table? Would adjusting these policies yield significant cost savings?**