Microsoft

Security Copilot in Intune Private Preview

Onboarding and Test Scenario Manual

V3.1

Microsoft

Welcome to the Security Copilot in Intune Private Preview

Welcome to the Private Preview!

Microsoft Security Copilot (Security Copilot) is a natural language, generative AI-powered security analysis tool that harnesses the full power of Microsoft Azure OpenAI architecture to help organizations do more. We are thrilled to extend this power to IT admins by integrating into the Microsoft Intune Admin Center.

This guide is designed to make your onboarding journey as smooth as possible by focusing your preview experience on a key set of Intune scenarios for IT administrators.

Here are a few onboarding items to get sorted out before you get started with the scenarios.

Onboarding – Part 1: Enable Security Copilot Early Access

After being notified by Microsoft that your account is ready, you must enable the Security Copilot in your tenant. Please refer to the online documentation for the step-by-step process, which includes selecting your geography:

Get started with Microsoft Security Copilot Early Access Program

https://learn.microsoft.com/en-us/security-copilot/get-started-security-copilot

Onboarding – Part 2: Prepare for the Intune Admin Center experience

After you complete Part 1 and Microsoft confirms that your Intune tenant has been "flighted" for the Intune private preview, you and other Intune administrators may start seeing "embedded" Copilot experiences appear in the Admin Center.

- **When we say "embedded," we're referring to Copilot calls to action (such as buttons, tooltips, and interactive icons) and work surfaces (such as context panes) that are available within Intune.**
- Other teams might use the phrase "inline" to refer to their experiences; we're still working on Microsoft-wide terminology.
- Another term you'll encounter in this guide is "skill," which refers to the underlying Copilot capability.

Before you start interacting with Copilot and attempting the scenarios in this document you should check these important things:

1. **Licensing:** There are no additional user licensing requirements for the Intune Private preview beyond those defined in the Early Access Program (EAP). The Intune private preview does not require any additional Defender or Entra ID licenses that are named as requirements in the online EAP documentation.
2. **User roles:** In addition to the roles required for the Security Copilot Standalone Early Access Program (https://learn.microsoft.com/en-us/security-copilot/get-started-security-copilot#assign-roles-to-users), Users should be assigned an Intune-specific role to access the Intune policy and device data. The "**Intune Administrator**" role provides access to read and create all Intune data and is therefore recommended for Private Preview. If your organization does not use the Intune Administrator role, you may use existing built-in or custom Intune roles, but be aware that Copilot will be limited by those permissions and scope tags. Please note that **all** users of the Intune portal will see the embedded Copilot UI, and it is not possible to hide those UI elements during the preview. **If you don't want all your admins to use Copilot, be sure to communicate that to your team.**

   To add the Intune administrator role to a user, go to the Entra portal , then navigate to Users > Roles.

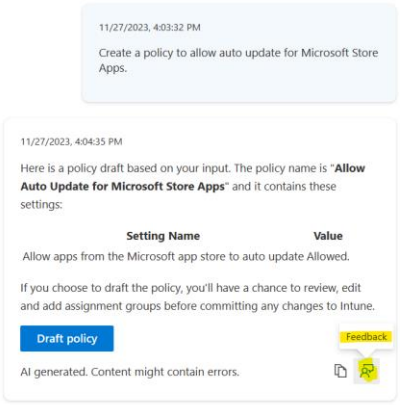
Microsoft

How and when to provide feedback to Microsoft

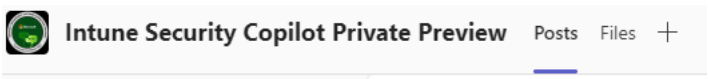
Please ensure that all users of the Intune embedded experience provide feedback regularly to help drive improvements in Copilot. Here are the key feedback mechanisms:

1. **Private preview scenario and summary feedback:** After you complete each scenario, you **must** complete a survey so we can collect your feedback. Scan the provided QR codes or follow the links at the end of each section to access the requisite surveys.

2. **In-product prompt output feedback:** At any point during the Private Preview, you can use the in-product feedback channel to confirm that Copilot gave you correct output, or to report incorrect or harmful output. To do this, use the feedback icon in the Intune embedded experience. Be descriptive with issues and expected results, particularly if you opted out of data sharing with Microsoft.



3. **Ask questions or report issues:** Use the Intune Security Copilot Private Preview Teams channel at any time to provide informal feedback, discuss your experiences, or ask questions. Note that the Teams channel doesn't replace the surveys! To ensure your voice is heard, you must complete those as well as use the in-product feedback experience.
   Link: Intune Security Copilot Private Preview



4. **Exit interviews:** We'll give you a chance to share your final thoughts on Intune embedded experiences as the Private preview program ends.

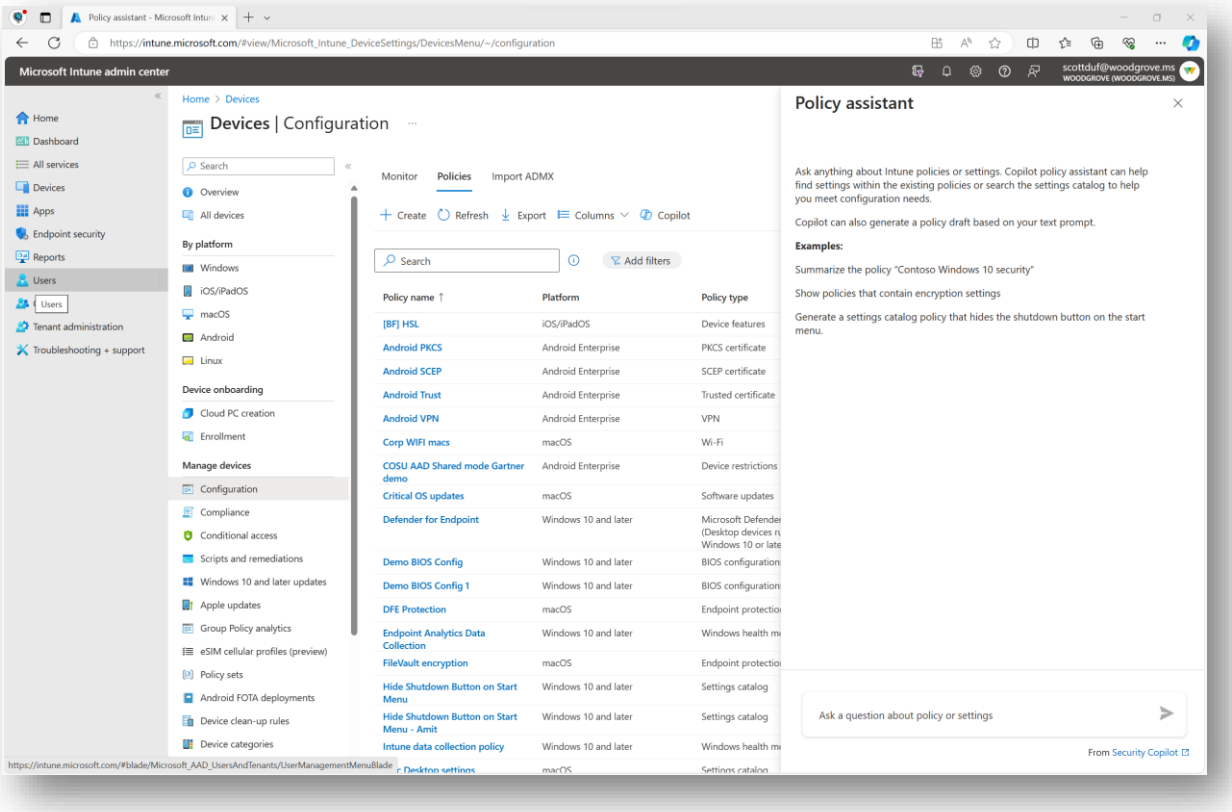
Test Scenarios:

Be sure to work your way through each scenario at least once. Upon completing each scenario, go to its associated survey and provide your feedback. This step is vital because it allows us to identify issues and improve the product.

Scenario 1: Create a policy using an open prompt

In this scenario, you will use natural language prompting in Security Copilot to generate a new Intune settings catalog policy object.

1. In the Intune portal, go to Devices > Configuration > Policies and select the "Copilot" button from the action bar.



2. A context pane opens. Use the open prompt field to try drafting an Intune settings catalog policy. Use "Generate" or "Draft" or "Create" as action words to ensure that Copilot calls upon the right policy creation capabilities. Here are some examples of working prompts:

Policy Generation sample prompts	Sample output
Create a policy that blocks users from using any removable storage devices on Windows 11 laptops	Here is the Intune configuration policy in JSON format that blocks users from using any removable storage devices on Windows 11 laptops. It contains the following settings: Setting Value All Removable Storage classes: Deny all access Enabled
Draft a BitLocker policy to require device encryption on system drive	Here is a policy draft based on your input. The policy name is "BitLocker System Drive Encryption Policy" and it contains these settings: Setting Name Value Require Device Encryption Enabled Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)Enabled Select the encryption method for operating system drives: XTS-AES 128-bit (default) If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy that enable windows SmartScreen for edge	Here is a policy draft based on your input. The policy name is "Enable Windows SmartScreen for Edge" and it contains these settings: Setting Name Value Configure Microsoft Defender SmartScreen Enabled If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create an Intune policy that turns on Windows firewall	Here is a policy draft based on your input. The policy name is "Enable Windows Firewall" and it contains these settings: Setting Name Value Enable Domain Network Firewall True Enable Private Network Firewall True Enable Public Network Firewall True If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Draft an account lockout Intune policy for Windows devices and set it to 3 failed attempts	Here is a policy draft based on your input. The policy name is "Account Lockout Policy" and it contains these settings: Setting Name Value Device Password Enabled Enabled Max Device Password Failed Attempts 3 If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Generate a policy to disable chrome extension in Microsoft Edge	Here is a policy draft based on your input. The policy name is "Disable Chrome Extensions in Microsoft Edge" and it contains these settings: Setting Name Value Allow Extensions Block If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy that does not show shut down from start menu.	Here is a policy draft based on your input. The policy name is "Hide Shut Down from Start Menu" and it contains these settings: Setting Name Value Hide Shut Down Enabled If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy that enable Smart Screen for edge.	Here is a policy draft based on your input. The policy name is "Enable Smart Screen for Edge" and it contains these settings: Setting Name Value Configure Microsoft Defender SmartScreen Enabled If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy that configures Microsoft auto update to enforce installation after 14 days on mac devices.	Here is a policy draft based on your input. The policy name is "Microsoft Auto Update 14 Days Enforcement" and it contains these settings: Setting Name Value Deferred updates Defer 14 days If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy to prevent autoplay on removable drives.	Here is a policy draft based on your input. The policy name is "Prevent Autoplay on Removable Drives" and it contains these settings: Setting Name Value Turn off Autoplay Enabled Turn off Autoplay on: CD-ROM and removable media drives If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.
Create a policy to allow auto update for Microsoft Store Apps.	Here is a policy draft based on your input. The policy name is "Allow Auto Update for Microsoft Store Apps" and it contains these settings: Setting Name Value Allow apps from the Microsoft app store to auto update Allowed.

	If you choose to draft the policy, you'll have a chance to review, edit and add assignment groups before committing any changes to Intune.

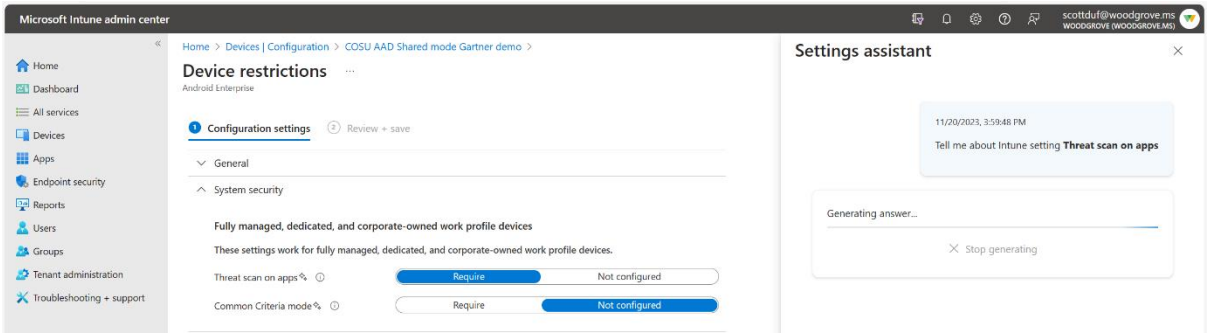
Tip:

- Use active verbs, such as “Generate,” “Draft,” or “Create” as keywords for the open prompt to invoke policy generation skills.

- The more context you provide an open prompt, the more accurate and complete the output will be. At present, Copilot does not proactively ask for additional insight before making inferences about your policy intent, **so provide it as much detail you can to make your desired outcome clear.**

- Did you run into an error? You can debug aspects of the prompt input, processing and output using the Security Copilot standalone experience. Go to Securitycopilot.microsoft.com and select the last session in your history to view more details on what went wrong.

3. Click the “Draft policy” button to enter the Policy creation wizard. The policy will have a name and description that you can edit if you want to, and each of the policy settings from the previous draft screen will be populated.
4. The settings are accompanied by Copilot icons, which usually appear next to the info icons. These icons invoke the Copilot Settings assistant. Click the icons for one or more of the settings. The prompt “Tell me about setting <settingname>” will be invoked in a context pane.



5. Now, use the Settings assistant to ask the questions below. **After Copilot generates an answer to each prompt, use the Feedback icon to tell us how it did.**
    a) How could this setting affect my users?
    b) How could this setting affect security?
    c) Has this setting been configured in any other policies?

d) Does Microsoft recommend any particular value for this setting?

6. Try using the open prompt to ask your own questions about the setting.
7. Click **Next** to advance to the next steps of the policy creation experience. Select any scope tags and assignment groups you want. When you arrive at the Review and Create wizard screen, select “Summarize policy” to invoke the Copilot context pane. It will be pre-populated with the starter prompt “Summarize this policy.”
8. Review the default output.
9. Try these additional suggested prompts:
    a) Describe the impact of this policy on users
    b) Describe the impact of this policy on Security
    c) Highlight setting conflicts with existing policy
10. Use an open prompt question , such as “Format the output in bullets instead of a table” to refine the preview results
11. Complete the survey for the “Create a policy from an open prompt” scenario.

Think about these questions when providing your feedback:

Did Copilot create the policy you expected?

Is the output something you can easily use for your internal change control documentation?

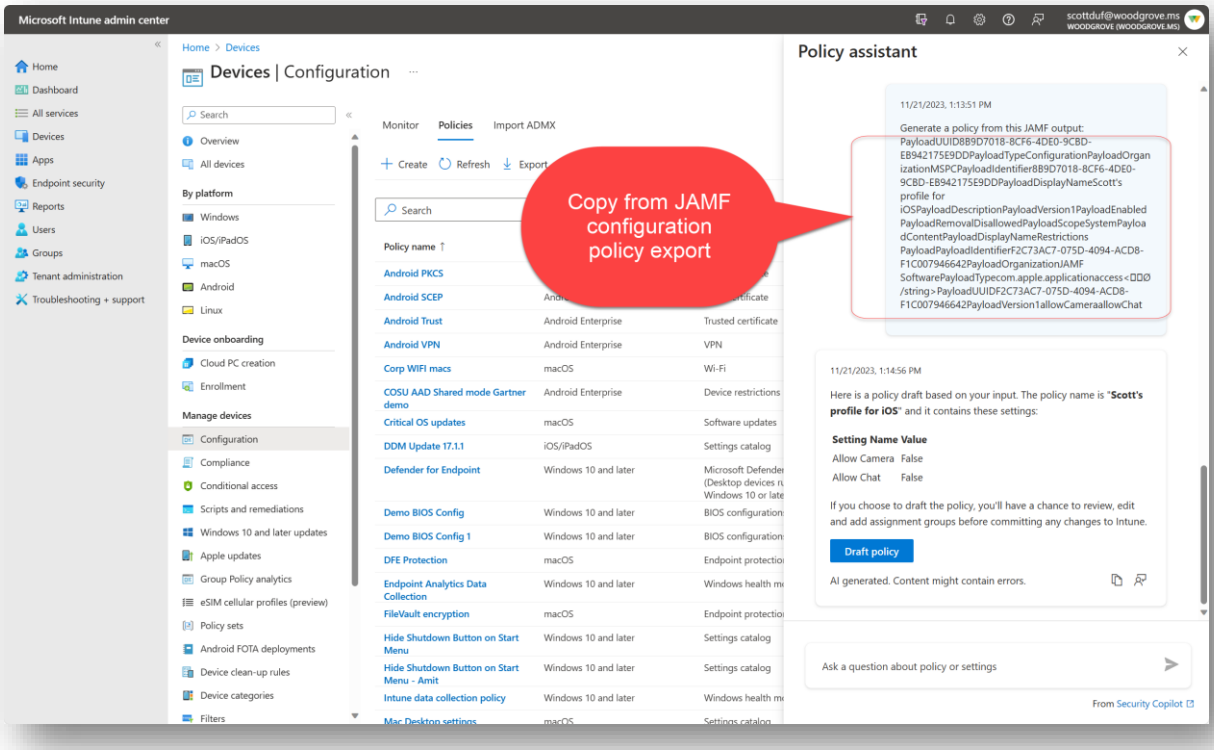
What changes would you like to see in the content of the output?

What additional data points would you like to know about when deploying a policy?

Scenario 2: Create a policy from a document

In this scenario you will provide Security Copilot with a rich document, which it will use as context to create a policy. Scenarios may include translating a policy object from another MDM product, an Excel spreadsheet, or another document.

1. In the Intune portal, go to Devices > Configuration > Policies and select the "Copilot" button from the action bar.
2. In the open prompt field, type "Generate a policy from" and paste additional text into the prompt. Here are some options:
    a) Export a policy from another MDM product. Open the policy with Notepad or another text viewer and copy the policy body into the prompt.
    b) Copy and paste Excel sheet settings and values cells from a document such as a security baseline.
    c) Choose another policy source that is applicable to your scenario.
3. Optional: Click "Draft policy," then review the policy with Copilot tooltips and summary features.
   Tip: It helps to tell Copilot what the source document is in the open prompt. For example, "Generate a policy from this JAMF output."



4. Complete the survey for the Create a Policy from a Document scenario.

5. 

Think about these questions when filling out the Private Preview feedback form:

Does the policy draft meet your expectations?

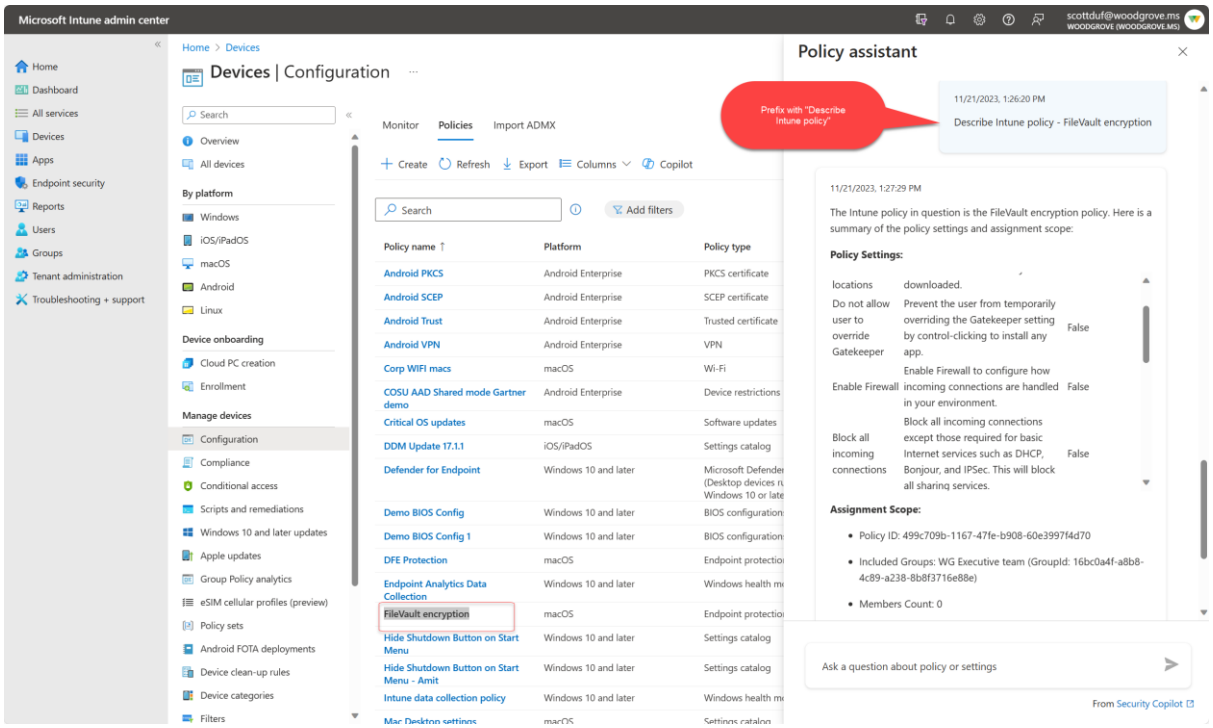
Are there any errors or missing settings?

What would you want to see changed in the overall policy draft experience?

Scenario 3: Summarize a policy

The previous two scenarios were all about new policies. This scenario exercises Copilot's ability to analyze existing policy objects saved in your environment and summarize them for you.

1. In the Intune portal, go to Devices > Configuration > Policies and select the "Copilot" button from the action bar.
2. Type an open prompt with a prefix string of "Describe Intune policy." For example, "Describe Intune policy - FileVault encryption."
3. Optional: Use the open prompt to adjust the output to your needs. For example, "Describe the impact on end users."



Tip:

There are limits on both the types of policies and the size of policies supported in Private preview. Please review the Known Issues and limitations section of this doc for further information.

4. Complete the survey for the Summarize a Policy scenario.

5.

Think about these questions when filling out the Private Preview feedback form:

Was the policy description what you expected?

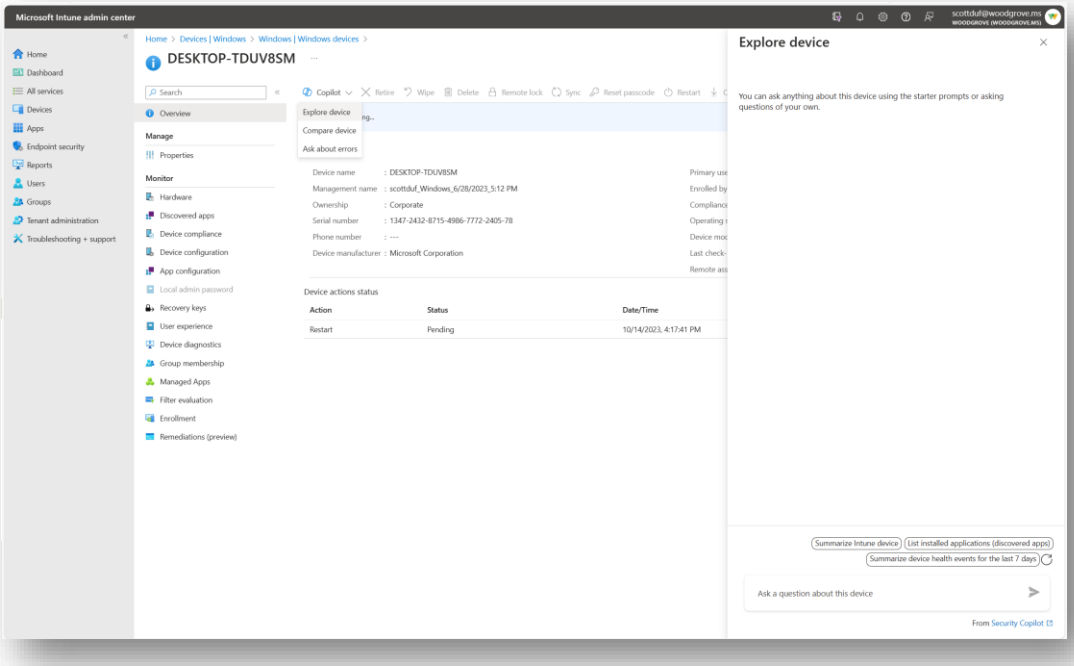
Was the formatting of the output what you expected?

Do you have any suggestions on how to improve this capability?

Scenario 4: Troubleshooting with Device Explorer

The following scenario uses Copilot to help you troubleshoot by answering questions about a given device.

1. Open the Intune portal at Intune.microsoft.com.
2. Go to Devices > All Devices and choose a device you are interested in exploring with Copilot.
3. From the Overview page, select Copilot > Explore device.



4. Attempt each of the suggested prompts from the table below. The table also details the specific skills invoked from each prompt and a sample output.

Prompt	Intune Skills	Sample output
Summarize Intune Device	GetIntuneDevices	*Here is a summary of the Intune device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba":* *Device Name: CPC-scott-GDMZ1* *Owner Type: company* *Managed Device Owner Type: company* *Management State: managed* *Enrolled Date: 2023-08-17T15:22:44.108942Z* *Last Sync Date: 2023-11-27T19:00:32.6008428Z* *Chassis Type: laptop* *Operating System: Windows* *Device Type: cloudPC* *Compliance State: compliant* *Jail Broken: Unknown* *Management Agent: mdm*

		OS Version: 10.0.22621.2715 *Azure AD Registered: true* *Device Enrollment Type: windowsAzureADJoin* *Model: Cloud PC Enterprise 2vCPU/8GB/128GB* *Manufacturer: Microsoft Corporation* *Azure AD Device Object ID: 4a0e9153-da96-4293-af02-c4395fe8d1cb* *Intune Device ID: 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba* *Primary User Information:* *Display Name: Scott Duffey* *User Principal Name: scottduf@woodgrove.ms* *User ID: d537e5f3-0a5a-49b1-96e7-531b801284a7* *Device Group Membership:* *The device is a member of 5 groups:* *Group ID: a16ef425-d460-44b5-a1e8-cbb00aa98e0c (Display Name not available)* *Group ID: faf3eb7c-a047-427d-86ae-1cb31a5013a4 (Display Name: All Cloud PC devices)* *Group ID: decbb526-5bcc-46cd-bbb5-447449ca241c (Display Name: LAPS-Devices)* *Group ID: b5a62a8f-9325-4299-878a-cba7bbae3fe9 (Display Name: ScottPC)* *Group ID: ac81e7c3-5d42-470f-935b-57b6a9e5c218 (Display Name: Engineering Laptops)*
Show me app installation failures	GetIntuneDeviceDiscoveredOrManagedApplication	For the device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba", there is a total of 1 managed app, and 1 has been processed. Here is the app installation information: | Application Name | Version | Installation Status | | ---------- | ------- | ---------- | | Notepad++ | | Installed | Please note that this information is for the primary user of the device. If you need more information, you can refer to the [Intune portal](https://intune.microsoft.com/).
Summarize device health events for the last 7 days	GetUserExperienceAnalyticsAppPerformanceReport	In the last 7 days, there have been several app crash and hang events reported for the device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba". Here is a summary of the events: - SenseNdr.exe (Microsoft) had multiple crashes with versions 2.3.1.0 and 2.4.0.7. - msteamsupdate.exe (Microsoft Corporation) had multiple crashes with version 23285.3703.2471.4627. - WaAppAgent.exe (Microsoft Corporation) had a crash with version 2.7.41491.1095. - MetricsExtension.Native.exe (Microsoft Corp.) had a crash with version 2.2021.426.1945-3957b8. - svchost.exe_AppXSvc (Microsoft Corporation) had a crash with version 10.0.22621.1. - MonAgentCore.exe (Microsoft Corporation) had a crash with version 45.5.2.0. - svchost.exe_DiagTrack (Microsoft Corporation) had a crash with version 10.0.22621.1. - SystemSettingsBroker.exe had a crash with no publisher and version information. - msedgewebview2.exe (Microsoft Corporation) had an app hang with version 118.0.2088.61. Please note that this information is based on Endpoint Analytics enrolled Windows devices on the tenant and the lookback duration is capped at 1 month.
Summarize device policy	GetPoliciesPerDevices	For the device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba", there are a total of 14 device configuration policies. Out of these, 7 policies have a status of Compliant, and none are in Error. The Compliant policies are: Defender for Endpoint Endpoint Analytics Data Collection Intune EPM Rules - M365 Installer Intune EPM Rules - PowerToys Intune EPM Settings Woodgrove standard configuration and security settings

		Woodgrove_Normal_Update Additionally, there are 3 device compliance policies for the device: Default Device Compliance Policy - Compliant Defender for Endpoint - Device Risk - Compliant PAW-Compliance-ATP - Not applicable There is no app configuration policy data available for the device. In summary, the device has a majority of its configuration policies in a Compliant state, and its compliance policies are either Compliant or Not applicable.
Who is the device's primary user	GetIntuneDevices	The primary user of the device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba" is Scott Duffey. His User Principal Name is scottduf@woodgrove.ms, and his User ID is d537e5f3-0a5a-49b1-96e7-531b801284a7.
List installed applications (Discovered apps)	GetIntuneDeviceDiscoveredOrManagedApplication	For the device with ID "8bdf1f63-dc6a-4e46-ad98-aae80e7560ba", there are a total of 60 discovered apps installed. However, only 50 apps have been processed due to a limit. Here is a list of the processed apps along with their versions: | Application Name | Version | | ---------- | ---------- | | Clipchamp.Clipchamp | 2.8.1.0 | | Global Secure Access Client | 1.6.51 | | Microsoft Cloud Managed Desktop Extension | 1.2.02481.194 | | Microsoft Edge | 119.0.2151.72 | | Microsoft Edge Update | 1.3.181.5 | | Microsoft Edge WebView2 Runtime | 119.0.2151.72 | | Microsoft Intune Management Extension | 1.72.115.0 | | Microsoft Update Health Tools | 5.72.0.0 | | Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 | 14.36.32532.0 | | Microsoft Windows Desktop Runtime - 6.0.25 (x64) | 6.0.25.33020 | | Microsoft.549981C3F5F10 | 4.2308.1005.0 | | Microsoft.BingNews | 4.55.62231.0 | | Microsoft.BingWeather | 4.53.52331.0 | | Microsoft.CompanyPortal | 11.2.179.0 | | Microsoft.DesktopAppInstaller | 2023.1005.18.0 | | Microsoft.EpmShellExtension | 1.0.0.0 | | Microsoft.GamingApp | 2309.1001.3.0 | | Microsoft.GetHelp | 10.2308.12552.0 | | Microsoft.HEIFImageExtension | 1.0.62561.0 | | Microsoft.HEVCVideoExtension | 2.0.61931.0 | | Microsoft.MicrosoftEdge.Stable | 119.0.2151.72 | | Microsoft.MicrosoftStickyNotes | 4.6.2.0 | | Microsoft.NET.Native.Framework.2.2 | 2.2.29512.0 | | Microsoft.NET.Native.Runtime.2.2 | 2.2.28604.0 | | Microsoft.OneDriveSync | 23209.1008.2.0 | | Microsoft.Paint | 11.2308.30.0 | | Microsoft.PowerAutomateDesktop | 10.0.7745.0 | | Microsoft.RawImageExtension | 2.1.62561.0 | | Microsoft.ScreenSketch | 2022.2309.16.0 | | Microsoft.SecHealthUI | 1000.25873.9001.0 | | Microsoft.Services.Store.Engagement | 10.0.23012.0 | | Microsoft.StorePurchaseApp | 22307.1401.9.0 | | Microsoft.Todos | 2.106.62642.0 | | Microsoft.UI.Xaml.2.7 | 7.2208.15002.0 | | Microsoft.UI.Xaml.2.8 | 8.2306.22001.0 | | Microsoft.VCLibs.140.00 | 14.0.32530.0 | | Microsoft.VCLibs.140.00.UWPDesktop | 14.0.32530.0 | | Microsoft.VP9VideoExtensions | 1.0.61591.0 | | Microsoft.WebMediaExtensions | 1.0.61591.0 | | Microsoft.WebpImageExtension | 1.0.62681.0 | | Microsoft.Windows.Photos | 2023.11090.12017.0 | | Microsoft.WindowsAppRuntime.1.2 | 2000.802.31.0 | | Microsoft.WindowsAppRuntime.1.3 | 3000.934.1904.0 | | Microsoft.WindowsCalculator | 2021.2307.4.0 | | Microsoft.WindowsFeedbackHub | 2023.504.1552.0 | | Microsoft.WindowsNotepad | 11.2307.27.0 | | Microsoft.WindowsSoundRecorder | 2021.2304.25.0 | | Microsoft.WindowsStore | 22309.1401.2.0 | | Microsoft.WindowsTerminal | 3001.18.2822.0 | | MicrosoftCorporationII.QuickAssist | 2023.531.2326.0 | Please note that this information is for the primary user of the device. If you need more information, you can refer to the [Intune portal](https://intune.microsoft.com/).

(Note: For each of the PROMPTS above, Intune prefixes "This device is [deviceID] in front of the text shown in the UI. When reviewing the prompt input and output in the standalone portal, the full prompt will be shown).

5. Use open prompting to try out additional Intune skills for single device troubleshooting. These are some prompts that can invoke additional capabilities:

Prompt	Skill
Who is assigned to my policy {policyname}	GetAppAndPolicyGroupTargetting
Summarize the group membership of my device	GetIntuneDeviceGroupMemberships
Show me the startup history for this device	GetUserExperienceAnalyticsDeviceStartupHistory
Show me startup processes that are impacting boot time for this device	GetUserExperienceAnalyticsStartupProcesses
Get user experience anomalies for this device	GetUserExperienceAnalyticsAnomaly
Get the device timeline for this device	GetIntuneDeviceTimelineEvents

6. Use open prompting to try out additional Intune skills for tenant-wide troubleshooting. These are some prompts that can invoke additional capabilities:

Prompt	Skill
Show me the devices enrolled by in the last 5 days	GetIntuneDevices
Give me the number of Intune applications with failed installations.	GetIntuneTenantFailedAppCount
How many Intune devices is app installed on?	GetIntuneTenantAppInstallationInfo
List all the device configuration policies for the tenant	GetIntuneTenantPolicyList
How many devices are not compliant?	GetIntuneTenantPolicyComplianceStatus
Which app has crashed on the most number of devices for my tenant?	GetUserExperienceAnalyticsAppPerformanceReport
On how many devices in the tenant is a setting {settingname} compliant?	GetIntuneTenantSettingComplianceStatus
Show me startup processes which are impacting boot time for all devices across the tenant	GetUserExperienceAnalyticsStartupProcesses
Which app has crashed on the most number of devices for my tenant?	GetUserExperienceAnalyticsAppPerformanceReport
What anomalies are we currently experiencing?	GetUserExperienceAnalyticsAnomaly
Give me all Intune devices with anomaly id '1961629613' and correlation Group id equal to '1245014848'	GetUserExperienceAnalyticsAnomalyDevices

1. Complete the survey for the “Troubleshoot with Device Explorer” scenario.

Think about these questions when filling out the Private Preview feedback form:

Was Copilot able to assist you in device troubleshooting? Why or why not?

Was the open prompt an effective method for asking about devices during troubleshooting?

Do you see a benefit of using Copilot instead of performing the task yourself through h the existing UI? Why or why not?

How can we improve the device troubleshooting experience with Copilot?

Scenario 5: Troubleshooting: Compare devices

When troubleshooting device issues, it can be helpful to compare a working/healthy device with a non-working/unhealthy device. In this scenario you’ll use Copilot to compare two Intune devices. This comparison can bring IT admins closer to uncovering the root cause of issues.

1. Open the Intune portal (Intune.microsoft.com)
2. Go to Devices > All Devices and choose a device you are interested in exploring with Copilot.
3. From the overview page, select Copilot > Compare device.
4. Use the open prompt to compare the currently selected device with another device in the tenant. The table below includes supported sample prompts:

Prompt	Skill	Sample output
Compare this device with DESKTOP-TDUV8SM. Show me the differences	GetIntuneDeviceDiff	Here is a comparison between the two devices, 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba and DESKTOP-TDUV8SM, focusing on their hardware differences: | Property | 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba | DESKTOP-TDUV8SM | |---|---|---| | Model | Cloud PC Enterprise 2vCPU/8GB/128GB | Virtual Machine | | PhysicalMemoryInBytes | 8,537,505,792 (8 GB) | 4,294,967,296 (4 GB) | | TotalStorageSpaceInBytes | 136,844,410,880 (128 GB) | 135,499,087,872 (126 GB) | | FreeStorageSpaceInBytes | 100,968,431,616 (94 GB) | 110,843,920,384 (103 GB) | ### Differences - The first device (8bdf1f63) is a Cloud PC Enterprise model with 2 vCPUs, 8 GB RAM, and 128 GB storage, while the second device (DESKTOP-TDUV8SM) is a Virtual Machine. - The first device has 8 GB of RAM, while the second device has 4 GB of RAM. - The first device has 128 GB of total storage space, while the second device has 126 GB of total storage space.

between hardware		- The first device has 94 GB of free storage space, while the second device has 103 GB of free storage space. ### Similarities - Both devices are manufactured by Microsoft Corporation. - Both devices run the Windows operating system. - Both devices have the same management agent (Mdm). - Both devices have the same device enrollment type (WindowsAzureADJoin) and device registration state (Registered). - Both devices have no specified device category and are not encrypted. ### Unique Properties - The first device has a compliant compliance state, while the second device has a noncompliant compliance state.

Compare this device with DESKTOP-TDUV8SM. Show me the differences between configuration policy	GetIntuneDeviceDiff	Here is a comparison of the configuration policies applied to the two devices, 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba and DESKTOP-TDUV8SM:
		
		### Similar Policies
		
		The following policies are applied to both devices:
		
		- Defender for Endpoint
		- Endpoint Analytics Data Collection
		- Intune EPM Rules - PowerToys
		- Intune EPM Settings
		- PAW-Win10-AppLocker-Custom-CSP
		- PAW-Win10-Config-Custom-CSP
		- PAW-Win10-Config-Device-Restrictions-UI
		- PAW-Win10-Config-Endpoint-Protection-UI
		- PAW-Win10-Config-Identity-Protection-UI
		- PAW-Win10-URLLockProxy-UI
		- PAW-Win10-Windows-Defender-Firewall-UI
		- Woodgrove_Normal_Update
		
		### Unique Policies
		
		The following policies are unique to each device:
		
		- Device 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba has the following unique policies:
		  - Intune EPM Rules - M365 Installer
		  - Woodgrove standard configuration and security settings
		
		- Device DESKTOP-TDUV8SM has the following unique policy:
		  - Bitlocker baseline config - scottduf
		
		In summary, both devices have a majority of similar policies applied, with only a few unique policies for each device.

Compare this device with DESKTOP-TDUV8SM. Show me the differences between compliance policy	GetIntuneDeviceDiff	Comparing the compliance policies between the two devices, we can observe the following differences and similarities: | Device ID | Policy Name | Compliance Status | UPN | |---|---|---|---| | 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba | Default Device Compliance Policy | Compliant | scottduf@woodgrove.ms | | 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba | Defender for Endpoint - Device Risk | Compliant | scottduf@woodgrove.ms | | 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba | PAW-Compliance-ATP | Not applicable | scottduf@woodgrove.ms | | DESKTOP-TDUV8SM | Default Device Compliance Policy | Not compliant | scottduf@woodgrove.ms | | DESKTOP-TDUV8SM | Defender for Endpoint - Device Risk | Compliant | scottduf@woodgrove.ms | | DESKTOP-TDUV8SM | PAW-Compliance-ATP | Not applicable | scottduf@woodgrove.ms | ### Similarities - Both devices have the same user (UPN: scottduf@woodgrove.ms). - Both devices have the same set of policies applied: Default Device Compliance Policy, Defender for Endpoint - Device Risk, and PAW-Compliance-ATP. - Both devices are compliant with the Defender for Endpoint - Device Risk policy. - Both devices have the PAW-Compliance-ATP policy marked as not applicable. ### Differences - The 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba device is compliant with the Default Device Compliance Policy, while the DESKTOP-TDUV8SM device is not compliant with the same policy.
Compare this device with DESKTOP-TDUV8SM. Show me the differences between	GetIntuneDeviceDiff	

Managed apps		
Compare this device with DESKTOP-TDUV8SM. Show me the differences between discovered apps	GetIntuneDeviceDiff	Here is a comparison of the discovered apps on the two devices, 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba and DESKTOP-TDUV8SM: For the device with ID 8bdf1f63-dc6a-4e46-ad98-aae80e7560ba, the following discovered apps have been found: | App Name | Version | |---|---| | Clipchamp.Clipchamp | 2.8.1.0 | | Global Secure Access Client | 1.6.51 | | Microsoft Cloud Managed Desktop Extension | 1.2.02481.194 | | Microsoft Edge | 119.0.2151.72 | | Microsoft Edge Update | 1.3.181.5 | | Microsoft Edge WebView2 Runtime | 119.0.2151.72 | | Microsoft Intune Management Extension | 1.72.115.0 | | Microsoft Update Health Tools | 5.72.0.0 | | Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 | 14.36.32532.0 | | Microsoft Windows Desktop Runtime - 6.0.25 (x64) | 6.0.25.33020 | | ... | ... | This device has a total of 60 discovered apps, and 50 have been processed due to a limit of 50 apps being shown. Unfortunately, I do not have information about the discovered apps for the DESKTOP-TDUV8SM device. Please provide more information or access to the device's discovered app data to compare the two devices.
Compare this device with DESKTOP-TDUV8SM. Show me the differences between App crashes	GetIntuneDeviceDiff	

(Note: For each of the PROMPTS above, Intune prefixes “This device is [deviceID]” to the prompt shown in the Intune UI. As a result, you only need to provide the second device to compare with and a comparison area. When debugging or reviewing the prompt input and output in the standalone portal, the full prompt will be displayed.)

Tip – Details on device comparison skills

The device comparison skill (GetIntuneDeviceDiffAsync) retrieves the differences or a comparison between two Intune devices for a specified category of data.

The skill requires several parameters as input:

Input 1: Device1 device name or Intune/aad device id

Input 2: Device2 device name or Intune/aad device id

Input 3: Aspect of the Intune device object that should be compared. Supported comparison vectors include Hardware configuration, Device configuration policies, App Configuration policies, Device compliance policies, App Crash data, Managed Apps installation data, Discovered apps data.

Input 4 (Optional): If comparing App crash information, you can specify the lookback schedule parameter (number of hours or days).

1. Complete the survey for the "Compare Devices" scenario.

Think about these questions when filling out the Private Preview feedback form:

Do Copilot's device comparison capabilities meet your expectations? Why or why not?

How can we improve the Copilot device comparison experience?

Scenario 6: Troubleshooting: Error code analysis

This scenario tests Copilot's ability to provide important information about error codes that IT admins find while troubleshooting devices in the Intune console. Note that for now, this skill is available only through the open prompt experience.

1. Open the Intune portal (Intune.microsoft.com)
2. Go to Devices > All Devices and choose a device you are interested in exploring with Copilot.
3. From the Overview page, select Copilot > Ask about errors
4. Use the open prompt to ask about errors that you are seeing for the device in the Intune console. The table below provides a sample to get you started.

Prompt	Skill
What does Intune error code 0xC7D14FB5 mean for a failed Android app installation?	ErrorCodeAnalyzer

5. Locate errors in your environment and ask about them using this experience. For example, you can navigate to the following areas of the Intune console to find codes and prompts to use:

a) Home> Apps > All apps > [App name] > Device Install status. Review the Status details columns for any error codes
b) Home> Devices> [Devicename]> Managed Apps > [App name]. Review the App installation failed details for one of the failed apps.
c) Home > Devices > [Devicename]>Configuration > [Device configuration policy name]. Review the Error code column for any failed settings within a configuration profile.

Tip – How to use open prompting with error code analyzer

The Intune skill (ErrorCodeAnalyzer) is currently designed to take an open prompt as input. The skill processes current Microsoft documentation to provide answers.

When using an open prompt with this skill, you should at a minimum include an error code (either hexadecimal or integer) to analyze, but should also add context that may help arrive at a more accurate prompt output.

For example, adding details such as the platform and the scenario will help.

6. Complete the survey for this scenario.

Think about these questions when filling out the Private Preview feedback form:

Did Copilot's error code analysis capabilities help you in troubleshooting? Why or why not?

How can we improve the Copilot error code analysis experience?

Final survey

Please complete this final survey to provide overall feedback.

Microsoft

Frequently asked questions

Does Copilot give my admins more access to Intune data that what they have using the UI?

No. The Intune skills available for preview are built on top of existing Microsoft Graph API's – the same API's that the Intune UI uses. This means that existing Intune permissions and scope tags will be respected by the Copilot while fetching data to answer a prompt. In the future, new API's may be created for additional capabilities and in those cases, new permissions may be added and configurable using Intune permissions and roles.

Is there any way to limit which Intune IT admins see the copilot experience during the preview?

No. During the private preview, all users of the Intune console will see the Copilot entry point show up. We are considering making controls available in product for GA. For the private preview, we recommend that customers communicate the private preview onboarding status with the entire team of Intune administrators and provide guidance on who should try it out.

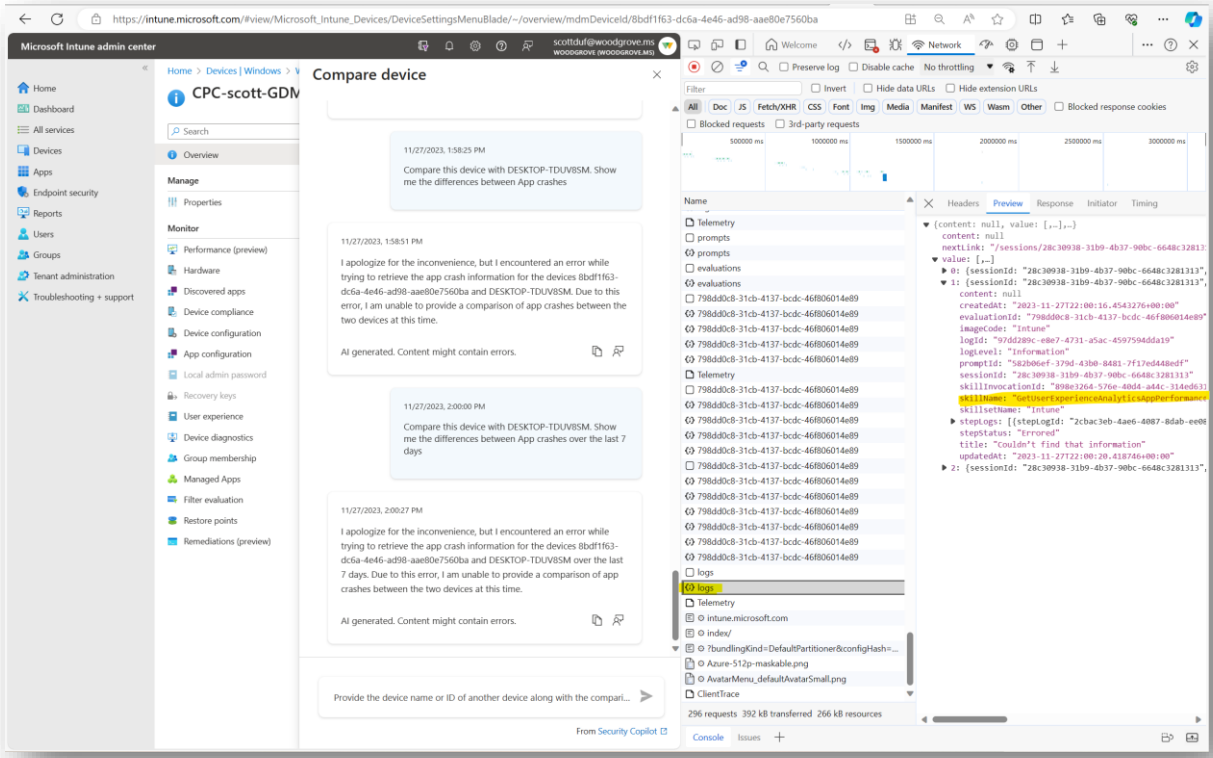
Can I leverage other Microsoft Security copilot capabilities from products such as Defender, Entra and Purview from within the Intune portal?

Currently the Intune embedded experience is limited to only Intune skills. Please provide feedback on skills that you would like to see from other products for further consideration.

Copilot is giving me what looks like the wrong answer to a prompt. How can I debug and validate this?

Firstly, if you suspect the output is incorrect, please use the embedded experience to provide feedback and add details about what you are seeing. If you are working with a Microsoft representative to debug the issue, they may ask you to enable F12 developer tools in your browser to validate the correct skill is being invoked by the Copilot skill orchestrator. Within the "network" view of Edge browser debug tools, you can use the

“Logs” entry to look more closely at the working steps between a prompt input and output.



Microsoft

Private preview limitations and known issues

Policy generation capabilities for Settings Catalog

1. Copilot is only able to generate Settings Catalog policy type at this point in time.
2. Copilot currently does not validate additional requirements for a policy generation prompt input. It does a one-time inference of policy intent.
3. Sometimes there is no “Draft Policy” button in the output.
4. Sometimes the configuration setting tab is empty after clicking “Draft Policy” button.

Policy Settings insights on Configuration Policies

1. Copilot settings insights are currently available on the following Intune configuration policy workloads:
    a. Settings catalog policies for all platforms
    b. All template-based configuration policies except Administrative Templates and OEMConfig profiles.
2. The skill currently does not make inferences about settings that have different names across policy types.
3. The answer for “Tell me about this setting” can retrieve unwanted sources and produce results from other Microsoft documentation sources outside Intune public docs. (Bug 13208)
4. Embedded tooltip button is not available on several policies where settings have no existing info balloon, for example:
    a. Configuration profiles->Ios/iPadOS->Templates-> Edition upgrade and mode switch
    b. Configuration profiles->Ios/iPadOS->Templates-> Secure assessment (Education)
    c. Configuration profiles->Windows 10 and later->Templates-> Administrative templates
5. Sometimes you may see the response “I’m sorry, but there is no information available about the setting named “Setting Name” in Configuration Profile, Compliance Policy, and Security Baseline. Please ensure that the setting name is correct or provide more context about the policy setting you are looking for.”
6. Sometimes you may see "The requested operation requires an element of type 'Object', but the target element has type 'Array'” when asking about settings usage.
7. Sometimes you may see the error "The given key was not present in the dictionary” when asking about settings usage.
8. For security baselines, if you click any link returned by a question about settings usage, you may be prevented from editing the policy setting.

9. You may see a starter prompt " What value do other customers configure for this setting?", which does not work.

Policy Summarization and What-if on Configuration policies

1. The skill (DescribeIntunePolicy) that supports summarization and what-if analysis is supported on the following workloads:
    a. Settings catalog policies
    b. Device configuration policies (templates), including Endpoint security but not including Security Baselines or Compliance policies.
2. The skill currently does not make inferences about settings that have different names across policy types.

Troubleshooting - General

1. Data limits – For all Intune troubleshooting skills, there is a row limit of 50 results for the output. For example, if an IT admin asks for all configuration policies impacting a given device, the copilot is capable of providing a total count of policies and displaying the first 50 only.

Troubleshooting - Comparing Devices

1. The device comparison skill (GetIntuneDeviceDiff) supports comparison of 7 vectors:
    a. Hardware config, App Policy, Device Compliance, Device config, Managed Apps, Discovered Apps, App Crash
    b. Managed and Discovered apps are currently limited to 50 apps per device.
2. For each vector, property elements are limited to the property columns on the admin portal

Troubleshooting - Error Code Analysis

1. The analysis skill (ErrorCodeAnalyzer) currently provides information on errors by leveraging Microsoft, Windows, Azure and Intune online documentation sources. Technical community docs pages or external blogs are currently not supported.
2. Some errors may be limited to a description only (unable to providing possible solutions/steps to troubleshoot) given the context of the document provided