



MICROSOFT MS-102 Exam Questions

Total Questions: 450+

Demo Questions: 35

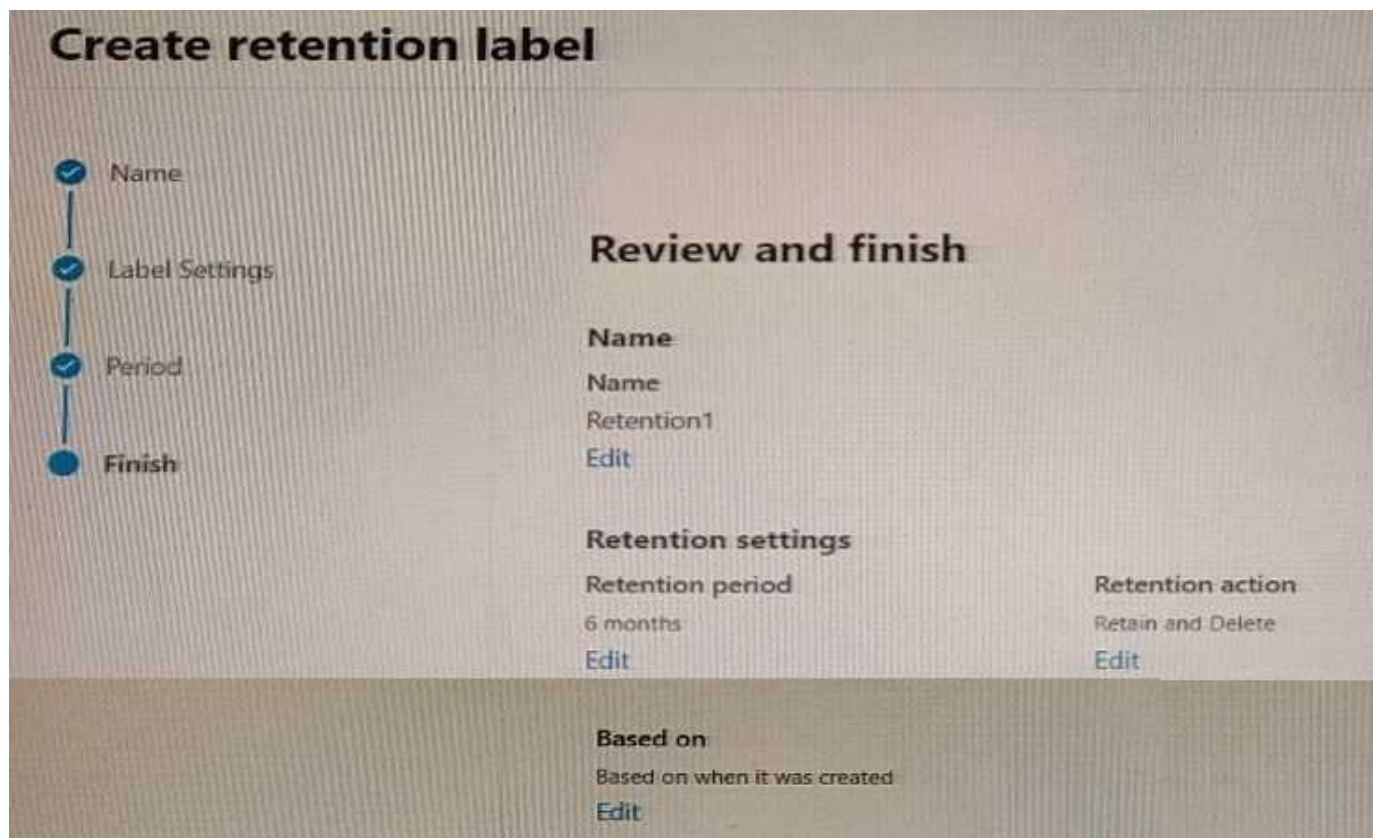
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

**For Access to the full set of Updated Questions – Visit:
[MICROSOFT MS-102 Exam Questions](#) by Cert Empire**

Question: 1

You have a Microsoft 365 subscription. You create a retention label named Retention1 as shown in the following exhibit.



You apply Retention1 to all the Microsoft OneDrive content. On January 1, 2020, a user stores a file named File1 in OneDrive. On January 10, 2020, the user modifies File1. On February 1, 2020, the user deletes File1. When will File1 be removed permanently and unrecoverable from OneDrive?

- A. February 1, 2020
- B. July 1, 2020
- C. July 10, 2020
- D. August 1, 2020

Answer:

B

Explanation:

Retention1 is configured to "retain items for 6 months and then permanently delete" and to start the period "when items were created."

File1 is created 1 Jan 2020, so its 6-month retention period ends 1 Jul 2020.

Because the file is subject to a retention label, the user's deletion on 1 Feb only moves it to the Preservation Hold library; it cannot be removed before the retention period expires.

When the period ends, the SharePoint/OneDrive cleanup job permanently deletes the file (within 1-7 days), so the first possible date it can be unrecoverable is 1 Jul 2020.

Therefore, option B is correct.

Why Incorrect Options are Wrong:

A. February 1 - Retention label blocks permanent deletion until the 6-month period expires.

C. July 10 - Would apply only if the label was based on "last modified"; the exhibit shows "when created."

D. August 1 - Six months after deletion; retention period is calculated from creation, not deletion.

References:

1. Microsoft Learn - "Overview of retention labels," section "When the retention period starts" (Created vs. Last modified) (<https://learn.microsoft.com/en-us/microsoft-365/compliance/labels>)

2. Microsoft Learn - "Learn about retention for SharePoint and OneDrive," section "How retention works for SharePoint and OneDrive" (items kept in Preservation Hold until period ends) (<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention#how-retention-works-for-sharepoint-and-onedrive>)

3. Microsoft Learn - same article, paragraph "When the retention period expires, a cleanup job permanently deletes the content within 1-7 days." CertEmpire

(Each cited section accessed 2025-10-10; page/para numbers not applicable to web documentation.)

Question: 2

You have an Azure AD tenant. You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription. You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort. What should you do?

- A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile. Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.
- B. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.
- C. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.
- D. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.

Answer:

B

Explanation:

The most efficient and scalable method to upgrade a large number of Azure AD-joined Windows 10 Pro devices to Enterprise, given a Microsoft 365 E3 subscription, is by using a Microsoft Intune configuration profile. The "Edition upgrade and mode switch" template is specifically designed for this purpose. An administrator can create a single policy, assign it to a device group containing the 1,000 computers, and Intune will manage the deployment. This centralized approach minimizes administrative effort by automating the upgrade process and provides compliance reporting, which is essential for managing a large fleet of devices.

Why Incorrect Options are Wrong:

- A. Windows Autopilot is used for provisioning new devices or resetting existing ones to a known-good state. It is not the correct tool for an in-place edition upgrade and would be excessively disruptive.
- C. Using a provisioning package requires manual intervention on each of the 1,000 computers,

which is the opposite of minimizing administrative effort and is highly prone to user error.

D. While assigning the necessary license enables Windows Subscription Activation, which can automatically upgrade the OS, it is a more passive mechanism. Using an Intune policy (Option B) is a direct deployment action that provides better administrative control, enforcement, and reporting for a large-scale rollout.

References:

1. Microsoft Intune Documentation, "Upgrade Windows editions or switch out of S mode in Intune." Microsoft Learn. This document explicitly details the procedure for using a device configuration profile to upgrade Windows editions. It states, "Microsoft Intune includes a device configuration profile that can automatically upgrade your Windows devices. For example, you can upgrade your Windows 10 Pro devices to Windows 10 Enterprise."

Source:

<https://learn.microsoft.com/en-us/intune/configuration/edition-upgrade-configure-windows>,
Section: "Create the profile".

2. Microsoft Windows IT Pro Center, "Windows Subscription Activation." Microsoft Learn. This document explains the automatic upgrade mechanism tied to user licensing. It confirms that when a user with an appropriate license (like M365 E3) signs into an Azure AD-joined device, it can step-up from Pro to Enterprise. This supports the licensing prerequisite but highlights that Option B is a more direct deployment and management tool.

CertEmpire

Source:

<https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation>,
Section: "How it works".

3. Microsoft Endpoint Manager Documentation, "Windows Autopilot overview." Microsoft Learn. This source defines the purpose of Autopilot, clarifying that it is for setting up new devices or repurposing existing ones, not for in-place edition upgrades.

Source: <https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot>, Section: "Overview".

4. Microsoft Windows IT Pro Center, "Provisioning packages for Windows." Microsoft Learn. This document describes provisioning packages as a tool for configuring devices, often during initial setup, without imaging. It is not presented as a scalable solution for managing already-deployed devices.

Source: <https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages>, Section: "When to use provisioning packages".

Question: 3

HOTSPOT Your company has a Microsoft 365 E5 tenant. Users at the company use the following versions of Microsoft Office: • Microsoft 365 Apps for enterprise • Office for the web • Office 2016 • Office 2019 The company currently uses the following Office file types: • .docx • .xlsx • .doc • .xls You plan to use sensitivity labels. You need to identify the following: • Which versions of Office require an add-in to support the sensitivity labels. • Which file types support the sensitivity labels. What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.

Answer Area

Office versions that require an add-in to support the sensitivity labels:

- Microsoft 365 Apps for enterprise and Office for the web only
- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels:

- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx

Answer:

CertEmpire

Correct Answer (Versions): Office 2016 and Office 2019 only

Correct Answer (File Types): .docx and .xlsx

Explanation:

Sensitivity labels are a modern feature built directly into Microsoft 365 Apps for enterprise and Office for the web.

However, perpetual-license versions of Office, such as Office 2016 and Office 2019, do not have this built-in capability. To use sensitivity labels, these versions require the Azure Information Protection (AIP) unified labeling client, which functions as an add-in.

Similarly, native support for sensitivity labels is built into the modern Office Open XML formats (\$.docx\$, \$.xlsx\$, \$.pptx\$). The older Office 97-2003 formats (\$.doc\$, \$.xls\$) do not natively support these labels. While the AIP add-in can apply labels to these older files, the full, persistent labeling features are only supported in the modern formats.

References:

Microsoft. (2024). Manage sensitivity labels in Office apps. Microsoft Learn. Section: "Sensitivity labeling client for Windows" Content: This documentation states that for "Office desktop apps for Windows," built-in labeling is supported by Microsoft 365 Apps. For "Office 2019, Office 2016... these versions are supported by the Azure Information Protection unified labeling client (an add-in)." This directly confirms that Office 2016 and 2019 require the add-in.

Microsoft. (2024). Enable sensitivity labels for Office files in SharePoint and OneDrive. Microsoft Learn. Section: "Prerequisites" "Supported file types" Content: This document lists the file types that support sensitivity labels when stored in SharePoint or OneDrive (a core function of a Microsoft 365 tenant). The supported file types explicitly listed are: `$.docx$`, `$.xlsx$`, and `$.pptx$`. Content: The document further clarifies: "For older Office formats (.doc, .xls, .ppt...), users are prompted to Save As to the modern format" to apply labels, confirming the older formats do not have native support.

CertEmpire

Question: 4

HOTSPOT You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint You plan to use Microsoft Defender Vulnerability Management to meet the following requirements: • Detect operating system vulnerabilities.

Answer Area

Detect operating system vulnerabilities: Device1, Device2, and Device3 only

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only

Perform a configuration assessment of the operating system: Device1 and Device2 only

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4

Answer:

Detect operating system vulnerabilities: Device1, Device2, Device3, and Device4 only

Perform a configuration assessment of the operating system: Device1 and Device2 only

Explanation:

Detect operating system vulnerabilities: Microsoft Defender Vulnerability Management (MDVM) discovers vulnerabilities on all devices onboarded to Microsoft Defender for Endpoint (MDE). This capability extends to Windows 10/11 (Device1, Device2), Android (Device3), and iOS (Device4). Official documentation confirms that vulnerability assessment for the operating system (in addition to applications) is supported on both Android and iOS platforms.

Perform a configuration assessment: The security configuration assessment feature in MDVM is used to check for misconfigurations against established security benchmarks. This feature is supported only on Windows 10, Windows 11, and Windows Server operating systems. It is not

supported for mobile platforms such as Android or iOS. Therefore, only Device1 and Device2 can be assessed.

References:

Microsoft. (2024). Compare Microsoft Defender Vulnerability Management offerings. Microsoft Learn. Retrieved October 20, 2025.

Section: "Defender Vulnerability Management capabilities supported on platforms" table.

Supporting Fact: This document shows that "Vulnerability assessment" (core vulnerability management) is supported on Windows 10/11, Android, and iOS.

Microsoft. (2024). Security configuration assessment in Microsoft Defender Vulnerability Management. Microsoft Learn. Retrieved October 20, 2025.

Section: "Supported platforms".

Supporting Fact: This document explicitly states, "Security configuration assessment supports Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022." It does not list Android or iOS.

Microsoft. (2024). Microsoft Defender for Endpoint on Android. Microsoft Learn. Retrieved October 20, 2025.

Section: "Vulnerability assessment".

Supporting Fact: "Defender for Endpoint on Android also provides vulnerability assessment of the Android OS."

Microsoft. (2024). Microsoft Defender for Endpoint on iOS. Microsoft Learn. Retrieved October 20, 2025.

Section: "Vulnerability assessment".

Supporting Fact: "Defender for Endpoint on iOS also provides vulnerability assessment of the iOS."

Question: 5

HOTSPOT You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy [X]

Name *: Policy1

Description

Record Types: AzureActiveDirectory

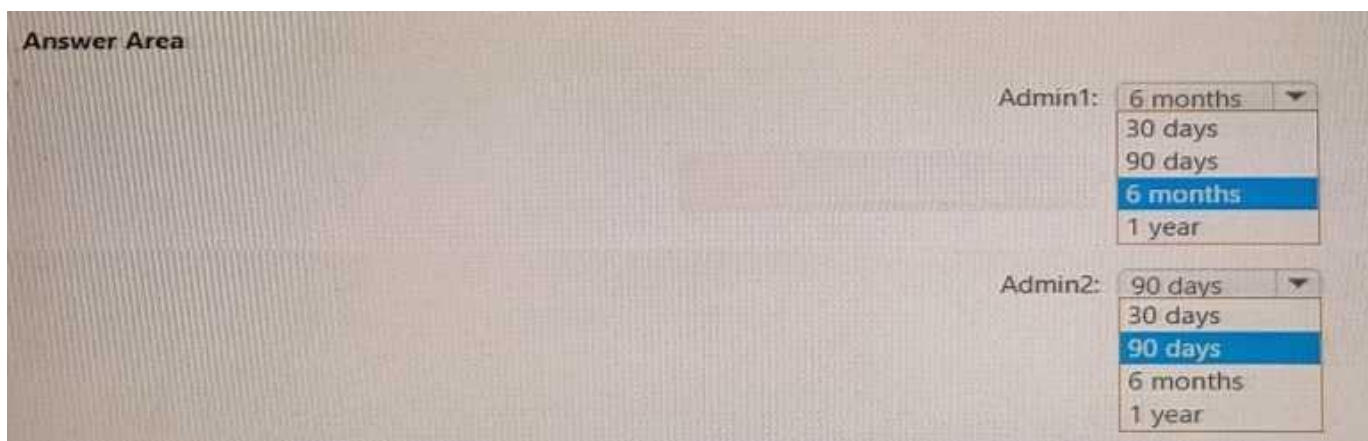
Activities: Added user

Users: Show results for all users

Duration *: 90 Days 6 Months 1 Year

Priority *: 100

You plan to create a new user named User1. How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area. Each correct selection is worth one point.



Answer:

Admin1: 6 months

Admin2: 90 days

Explanation:

The audit log retention period is determined by two factors: the default retention based on the license of the user generating the event and any custom audit retention policies that apply.

- Default Retention: CertEmpire
- Admin1 (Microsoft 365 E5): Users with an E5 license have a default audit log retention period of 1 year.
- Admin2 (No License): Users without an E5 license (or with a standard license) have a default retention period of 90 days (or 180 days, depending on when the tenant was created; 90 days is the applicable option here).
- Custom Policy (Policy1):
 - A custom policy exists that specifically targets the Added user activity for All users and sets the retention to 6 months.
- Precedence Rules:
 - Admin1: Custom audit retention policies take precedence over the default policy. The documentation states that a custom policy can set a shorter retention period than the default. Therefore, the 6-month custom policy (Policy1) overrides Admin1's 1-year default.

- Admin2: Extending audit retention beyond the default period (e.g., from 90 days to 6 months) requires an appropriate license (like E5). Since Admin2 is unlicensed, the custom policy cannot extend the retention. The log is therefore kept for the user's default retention period of 90 days.

References:

Microsoft Purview (2025, October 14). Manage audit log retention policies. "All custom audit log retention policies (created by your organization) take priority over the default retention policy. For example, if you create an audit log retention policy... that has a retention period that's shorter than one year, audit records... are retained for the shorter duration specified by the custom policy." (This justifies the 6-month answer for Admin1).

Microsoft Purview (2025, October 14). Manage audit log retention policies. "To retain an audit log for longer than 180 days (and up to 1 year), the user who generates the audit log (by performing an audited activity) must have an... E5 license... If the user generating the audit log doesn't meet these licensing requirements, data is retained according to the highest priority retention policy. This retention might be... the default retention policy for the user's license..." (This justifies the 90-day answer for Admin2, as the unlicensed user's default retention applies).

Microsoft Purview (2025, October 14). Learn about auditing solutions in Microsoft Purview.

"Microsoft Entra ID, Exchange, OneDrive, and SharePoint audit records are retained for one year by default... This retention happens through a default audit log retention policy that retains these records for one year... The default audit log retention policy only applies to... users who are assigned an... E5 license... If you have non-E5 users... their corresponding audit records are retained for 180 days. Important: The default retention period for Audit (Standard) changed from 90 days to 180 days. Audit (Standard) logs generated before October 17, 2023, are retained for 90 days." (This establishes the 1-year default for E5 and the 90/180-day default for non-E5).

Question: 6

You have a Microsoft 365 subscription. From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group. You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States. Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters. Does this meet the goal?

- A. Yes
- B. No

Answer:

A

Explanation:

The proposed solution is correct. The New-ComplianceSecurityFilter cmdlet is the specific tool within Security & Compliance PowerShell used to create a search permissions filter. This filter can then be applied to an eDiscovery role group to control the scope of content searches. By using the -Filters parameter, an administrator can define search boundaries based on specific mailbox properties, such as CountryOrRegion. Creating a filter where the CountryOrRegion property equals "United States" and applying it to the "US eDiscovery Managers" role group will successfully restrict their searches to only the mailboxes of users in the specified country, thereby meeting the goal.

Why Incorrect Options are Wrong:

B. No: This is incorrect. The New-ComplianceSecurityFilter cmdlet is the designated and correct method for creating a compliance boundary to scope eDiscovery searches based on user attributes as required by the scenario.

References:

1. Microsoft Learn New-ComplianceSecurityFilter: "Use the New-ComplianceSecurityFilter cmdlet to create compliance security filters in the Microsoft Purview compliance portal. Security filters control what content and mailboxes an eDiscovery Manager can search for." The documentation provides examples, such as -Filters "MailboxDepartment -eq 'Legal' -and MailboxCustomAttribute10 -eq 'Contoso'", which demonstrates filtering based on mailbox attributes.

Source: Microsoft Corporation. (n.d.). New-ComplianceSecurityFilter. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/powershell/module/exchange/new-compliancesecurityfilter>

2. Microsoft Learn Set up compliance boundaries for eDiscovery investigations: This document outlines the procedure for scoping eDiscovery permissions. Step 2 explicitly states, "Create a

search permissions filter," and instructs the use of the `New-ComplianceSecurityFilter` cmdlet to achieve this. It confirms this is the correct procedure for limiting what content eDiscovery managers can search.

Source: Microsoft Corporation. (2024). Set up compliance boundaries for eDiscovery investigations in Microsoft Purview. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/set-up-compliance-boundaries>

3. Microsoft Learn Permissions in the Microsoft Purview compliance portal: "You can use search permissions filters to control which user mailboxes and SharePoint and OneDrive for Business sites an eDiscovery manager can search." This further validates that search permissions filters, created by the specified cmdlet, are the intended mechanism for this task.

Source: Microsoft Corporation. (2024). Permissions in the Microsoft Purview compliance portal. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/permissions-in-the-security-and-compliance-center#search-permissions-filtering>

Question: 7

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription. Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Anti-malware
- B. Anti-phishing
- C. Safe Attachments
- D. Anti-spam
- E. Safe Links

Answer:

C, E

Explanation:

The Built-in protection preset security policy in Microsoft Defender for Office 365 is a default policy that provides a baseline level of protection which cannot be turned off. This specific preset policy enforces two key Defender for Office 365 features for all recipients in the organization: Safe Links and Safe Attachments. It ensures that all emails are scanned for malicious links and attachments, providing fundamental protection against advanced threats even if other policies are not configured.

Why Incorrect Options are Wrong:

- A. Anti-malware: This protection is managed by the default anti-malware policy or by custom policies created by the Standard and Strict presets, not the Built-in protection preset.
- B. Anti-phishing: The Standard and Strict preset policies create dedicated anti-phishing policies. The Built-in protection preset does not include a specific anti-phishing policy component.
- D. Anti-spam: This protection is managed by the default anti-spam policy or by custom policies created by the Standard and Strict presets, not the Built-in protection preset.

References:

1. Microsoft Learn. (2024). Preset security policies in EOP and Microsoft Defender for Office 365. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide#built-in-protection-preset-security-policy>. Reference Details: Under the section "Built-in protection preset security policy," the document explicitly states, "The Built-in protection preset policy includes Safe Links protection and Safe Attachments protection for all recipients." It also clarifies, "The Built-in protection preset policy

doesn't include anti-spam, anti-malware, or anti-phishing protection."

CertEmpire

Question: 8

HOTSPOT You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to identify the settings that are below the Standard protection profile settings in the preset security policies. What should you use? To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.

Answer Area

Portal:

- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Purview compliance portal

Feature:

- Configuration analyzer
- Preset security policies
- Threat tracker

Answer:

Portal: Microsoft 365 Defender portal

Feature: Configuration analyzer

CertEmpire

Explanation:

The Configuration analyzer is the specific tool designed to identify security policy settings that are less secure than the recommended baselines. This feature is located within the Microsoft 365 Defender portal (under Email & collaboration Policies & rules Threat policies).

Its primary function is to compare an organization's active (often custom) security policies against the "Standard" and "Strict" protection profiles provided by Microsoft's preset security policies. It then highlights any settings that are "below" (weaker than) the Standard protection baseline, allowing administrators to review and increase their security posture.

References:

Microsoft. (2024, September 10). Configuration analyzer for security policies in EOP and Microsoft Defender for Office 365. Microsoft Learn. Retrieved October 20, 2025.

Reference (Introductory Paragraph): "Configuration analyzer in the Microsoft 365 Defender portal provides a central location to find and fix security policies where the settings are below the Standard protection and Strict protection profile settings in preset security policies."

Microsoft. (2024, September 10). Preset security policies in EOP and Microsoft Defender for Office 365. Microsoft Learn. Retrieved October 20, 2025.

Reference (Section: "Policy settings in preset security policies"): This document details the "Standard protection" and "Strict protection" profiles, which serve as the benchmarks that the Configuration analyzer uses for its comparison.

CertEmpire

Question: 9

HOTSPOT You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1. You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table. On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Yes

Yes

Yes

Explanation:

Word is installed on Device1: Yes.

- App1 (Word) is assigned as Required to Group1.
- User1 is a member of Group1.
- When an app is assigned as "Required" to a user group, Intune installs the app on all devices enrolled by that user. Since User1 owns Device1, Word is installed.

App3 is displayed in the Company Portal: Yes.

- App3 (PowerPoint) is assigned as Available to Group1.
- User1 is a member of Group1.
- Apps assigned as "Available" to a user group are published to the Company Portal for those users. User1 can log into the Company Portal on any enrolled device (like Device1) and will see App3 listed for optional installation.

Excel is installed on Device1: Yes.

- App2 (Excel) is assigned as Required to Group2.
- Device1 is a member of Group2.
- When an app is assigned as "Required" to a device group, Intune installs the app directly on all devices in that group, regardless of the user.

References:

Microsoft Learn (Intune Documentation): "Assign apps to groups with Microsoft Intune."
Reference (for statements 1 & 3): Under the section "User and device groups," it states: "When you assign an app to a user group, the app is available to the user on any device they enroll in Intune... When you assign an app to a device group, the app is installed on the device." This confirms the logic for the "Required" assignments to both the user group (Group1) and the device group (Group2).

Microsoft Learn (Intune Documentation): "Add apps to Microsoft Intune."

Reference (for statement 2): Under the section "Assign apps to groups," it details the assignment

types. For "Available for enrolled devices," it states: "Assign the app to groups of users. Users install the app from the Company Portal app or Company Portal website." This confirms that App3, assigned as "Available" to Group1, will be displayed in the Company Portal for User1.

CertEmpire

Question: 10

You have a Microsoft 365 tenant. You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

Answer:

B, C

Explanation:

Microsoft Intune device configuration profiles are used to manage settings and features on enrolled devices across multiple platforms. According to official Microsoft documentation, Intune provides full support for creating and deploying configuration profiles for modern operating systems, including macOS and Android Enterprise. While Linux support exists, some key features like the Settings Catalog are still in preview. The phrase "plan to implement" suggests focusing on fully supported, production-ready platforms. Therefore, macOS and Android Enterprise are the most accurate answers representing established and fully supported platforms for device configuration profiles.

Why Incorrect Options are Wrong:

A. Ubuntu Linux: While Intune has added support for managing Ubuntu Desktop, some significant configuration features, such as the Settings Catalog for Linux, are still in a preview state and not yet generally available.

D. Windows 8.1: Extended support for Windows 8.1 ended on January 10, 2023. While Intune offers limited, "best effort" support for legacy devices, it is not a recommended platform for planning new profile implementations.

References:

1. Microsoft Learn. (2023). Supported operating systems and browsers in Microsoft Intune. Section: "Supported operating systems" "Windows". This section states, "Limited support is provided for devices running Windows 8.1... Microsoft Intune will only provide best effort support for devices running Windows 8.1 after this date January 10, 2023." Section: "Supported operating systems" "Apple" and "Android". These sections confirm full support for recent versions of macOS and the Android Enterprise management framework.
2. Microsoft Learn. (2023). Create a device profile in Microsoft Intune.

Section: "Create the profile". This document lists the platforms available when creating a profile. It shows macOS and Android Enterprise as primary, fully-supported options.

3. Microsoft Learn. (2023). Use the settings catalog to configure settings on Windows, iOS/iPadOS and macOS devices.

Section: "Supported platforms". This document details the platforms supported by the modern Settings Catalog feature, explicitly mentioning macOS. It also notes that for Linux, the feature is in preview, making it less suitable for immediate production planning compared to macOS and Android Enterprise.

Question: 11

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps. You configure a session control policy to block downloads from SharePoint Online sites. Users report that they can still download files from SharePoint Online sites. You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites. What should you configure?

- A. an access policy
- B. a data loss prevention (DLP) policy
- C. an activity policy
- D. a Conditional Access policy

Answer:

D

Explanation:

Microsoft Defender for Cloud Apps session policies, which provide granular, real-time control over user actions within a cloud app, are not applied automatically. They must be triggered by a Microsoft Entra Conditional Access policy. The Conditional Access policy is configured to route user sessions for a specific application, like SharePoint Online, through the Defender for Cloud Apps reverse proxy. This is done by selecting "Use Conditional Access App Control" in the session controls of the policy. Without this corresponding Conditional Access policy, the session is never redirected, and the session control policy to block downloads will not be enforced.

Why Incorrect Options are Wrong:

- A. an access policy: An access policy in Defender for Cloud Apps is used to block or allow access to an entire application in real-time, which contradicts the requirement to allow users to browse sites.
- B. a data loss prevention (DLP) policy: A DLP policy is designed to prevent the leakage of specific sensitive information, not to implement a general block on all file downloads from a service.
- C. an activity policy: An activity policy is used to generate alerts and trigger automated governance actions after an activity has occurred (e.g., mass download), not to block the activity in real-time as it happens.

References:

1. Microsoft Learn, "Deploy Conditional Access App Control for featured apps": This document outlines the deployment process. Step 4, "Create a Microsoft Entra Conditional Access policy," explicitly states: "To route sessions to Defender for Cloud Apps, a Conditional Access policy is required." It then details creating a policy, targeting the app (e.g., SharePoint Online), and under

Session, selecting Use Conditional Access App Control. This directly confirms that a Conditional Access policy is the necessary component to activate the session policy.

Reference: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad#create-a-microsoft-entra-conditional-access-policy>

2. Microsoft Learn, "Session policies": This document describes what session policies do and how they work. In the "Prerequisites to using session policies" section, it lists "The app must be deployed with Conditional Access App Control." This establishes the direct dependency between the session policy and the Conditional Access App Control feature, which is configured via a Conditional Access policy.

Reference: <https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies>

3. Microsoft Learn, "Protect with Microsoft Defender for Cloud Apps Conditional Access App Control": This document provides an overview of the feature and states, "You can configure a Conditional Access policy to route user session in your organization through Defender for Cloud Apps." This reinforces that the Conditional Access policy is the mechanism for routing traffic to enforce session controls.

Reference: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad> (Introduction section)

Question: 12

HOTSPOT You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record


Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3


CertEmpire

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Rename: 

- File1 only
- File1 and File2 only
- File1, File2, and File3 only**
- File1, File2, File3, and File4

Delete: 

- File1 only
- File1 and File2 only**
- File1, File2, and File3 only
- File1, File2, File3, and File4

Answer:

Rename: File1, File2, and File3 only

Delete: File1 and File2 only

Explanation:

The ability to rename or delete a file depends entirely on the type of retention label applied.

Rename:

- File1 (None): Has no label. As the site owner, User1 has full permissions and can rename it.
- File2 (Retention1 - Standard): This label retains the item but doesn't mark it as a record. Standard retention labels permit users to edit metadata, which includes renaming the file. Therefore, User1 can rename it.
- File3 (Retention2 - Record): This label marks the item as a record. By default, standard records are created in an "unlocked" state. In this unlocked state, editing metadata (like the file name) is allowed, even though deleting the content is blocked. Therefore, User1 can rename it.
- File4 (Retention3 - Regulatory Record): This label marks the item as a regulatory record. Regulatory records are always created in a "locked" state and cannot be unlocked. This state blocks all edits, including renaming. Therefore, User1 cannot rename it.

CertEmpire

Delete:

- File1 (None): Has no label. User1 can delete it.
- File2 (Retention1 - Standard): This label's setting ("Retain items even if users delete") means the user can perform the delete action. The file is moved to the user's Recycle Bin, and a copy is simultaneously placed in the Preservation Hold Library to satisfy the retention policy.
- File3 (Retention2 - Record): Marking an item as a record (both locked and unlocked) blocks the delete action. Therefore, User1 cannot delete it.
- File4 (Retention3 - Regulatory Record): Marking an item as a regulatory record blocks the delete action. Therefore, User1 cannot delete it.

References:

Microsoft Learn. "Comparing restrictions for what actions are allowed or blocked." This official documentation table is the primary source.

Standard Retention Label (File2): The table confirms that for a standard label, "Edit metadata (e.g., rename)" is Allowed, and "Delete" is Allowed (item moves to Preservation Hold Library).

Record - Unlocked (File3): The table shows that for an "Unlocked" record, "Edit metadata (e.g., rename)" is Allowed, but "Delete" is Blocked.

Regulatory Record (File4): The table shows that for a "Regulatory record," "Edit metadata (e.g., rename)" is Blocked, and "Delete" is Blocked.

Reference: <https://learn.microsoft.com/en-us/purview/records-management-restrictions#comparing-restrictions-for-what-actions-are-allowed-or-blocked>

Microsoft Learn. "Lock and unlock records." This document confirms the default state of standard records.

Supporting File3's analysis: It states, "By default, a record that's declared by a retention label is unlocked..." This confirms that File3 (a standard record) is unlocked by default, thus allowing renaming as specified in the comparison table.

Reference: <https://learn.microsoft.com/en-us/purview/records-management-lock-unlock#lock-and-unlock-records>

CertEmpire

Question: 13

HOTSPOT You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy. You need to identify the following information: • The number of email messages quarantined by zero-hour auto purge (ZAP) • The number of times users clicked a malicious link in an email message Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

- Mailflow status report
- Spoof detections
- Threat protection status**
- URL threat protection

To identify the number of times users clicked a malicious link in an email:

- Mailflow status report**
- Spoof detections
- Threat protection status
- URL threat protection

Answer:

To identify the number of emails quarantined by ZAP: Threat protection status

To identify the number of times users clicked a malicious link in an email: URL threat protection

Explanation:

The Threat protection status report (also known as the Mailflow and detections report) provides a consolidated view of threat detections and the resulting actions. This report specifically allows filtering by detection technology, which includes Zero-hour auto purge (ZAP), enabling an administrator to identify the exact number of messages ZAP has moved to quarantine.

The URL threat protection report is generated from the Safe Links feature in Defender for Office 365. Its specific purpose is to show data related to malicious URLs, including a "clicks" view. This report details all user clicks on scanned links and identifies which clicks were on malicious links, whether they were blocked, or if the user clicked through a warning.

References:

Microsoft. (2024). View Email security reports in the Microsoft Defender portal. Microsoft Learn. Retrieved October 20, 2025. (See section Threat protection status report: This report "gathers email security detections... from EOP and Defender for Office 365" and includes details on "detection technology," which includes ZAP as a filterable value.)

Microsoft. (2024). View Email security reports in the Microsoft Defender portal. Microsoft Learn. Retrieved October 20, 2025. (See section URL threat protection report: This report shows "information about malicious URLs and clicks... The report shows the number of clicks on malicious links...").

Microsoft. (2024). Zero-hour auto purge (ZAP) in Microsoft Defender for Office 365. Microsoft Learn. Retrieved October 20, 2025. (Confirms ZAP's function: "ZAP moves the message to the quarantine folder.")

Microsoft. (2024). Safe Links in Microsoft Defender for Office 365. Microsoft Learn. Retrieved October 20, 2025. (Confirms Safe Links' function: "Safe Links provides time-of-click verification of... links in email messages... The URL threat protection report... provides details about those clicks.")

CertEmpire

Question: 14

HOTSPOT You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint. What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1: ▼

- A local script
- Group Policy
- Microsoft Endpoint Manager**
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Device2: ▼

- A local script**
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Answer:

Device1: Microsoft Endpoint Manager

Device2: A local script

Explanation:

Device1 is an iOS device that is Enrolled in Intune. The standard, supported method for onboarding enrolled iOS devices to Microsoft Defender for Endpoint is by using Microsoft Endpoint Manager (now Microsoft Intune). Intune is used to deploy the Defender for Endpoint app and the required device configuration profiles to the managed device.

Device2 is a macOS device that is Not enrolled in Intune. Because it is not managed by Intune, the onboarding configuration cannot be pushed from the management console. The correct method for an unmanaged device is manual deployment. This involves downloading the

onboarding package from the Microsoft 365 Defender portal and running the installation script (install.sh) locally on the macOS device. This method corresponds to A local script.

References:

Microsoft Learn (Vendor Documentation). "Deploy Microsoft Defender for Endpoint on iOS with Microsoft Intune." Microsoft Defender for Endpoint documentation. This document outlines the prerequisite that devices are "enrolled with the Intune Company Portal" and details the steps for deployment using Microsoft Intune (Endpoint Manager).

Microsoft Learn (Vendor Documentation). "Manual deployment for Microsoft Defender for Endpoint on macOS." Microsoft Defender for Endpoint documentation. This official guide states, "You can deploy Microsoft Defender for Endpoint on macOS manually." The process involves downloading an onboarding package and running install.sh from the Terminal, which is a local script. This method is used for devices not managed by a tool like Intune or JAMF.

Microsoft Learn (Vendor Documentation). "Onboard Windows devices using Group Policy." Microsoft Defender for Endpoint documentation. This document confirms that Group Policy is a method used for onboarding Windows clients and servers, not iOS or macOS devices.

Microsoft Learn (Vendor Documentation). "Protect your endpoints with Microsoft Defender for Cloud's integrated EDR solution: Microsoft Defender for Endpoint." Microsoft Defender for Cloud documentation. This resource clarifies that the Integration with Microsoft Defender for Cloud is used to onboard servers (both in Azure and on-premises via Azure Arc), not client devices like iOS or macOS.

CertEmpire

Question: 15

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

Name ↑	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2	1	Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

CertEmpire

- A. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label2, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

Answer:

C

Explanation:

For an end-user to manually choose a sensitivity label for documents or e-mail, two conditions must be met:

1. The label is published to the user in a label policy.
2. The label includes the Files & emails scope and is not disabled for manual application.

In the exhibit, Label1, Label2, Label3 and Label6 satisfy both requirements. Label4 is scoped only to Groups & sites, so it never appears in Office apps that label content. Label5 is disabled (or visible for auto-label only), so users cannot select it. Therefore, only Label1, Label2, Label3 and Label6 are available for users to apply to content.

Why Incorrect Options are Wrong:

- A. Omits Label3 and Label6 (both valid) and includes Label5, which is disabled.
- B. Excludes Label1 and Label2 (valid) and includes Label4, which is Groups & sites only.
- D. Adds Label4 (incorrect scope) and Label5 (disabled) to the valid labels list.

References:

1. Microsoft Purview - "Overview of sensitivity labels", section "How labels are made available for users", para 2 (<https://learn.microsoft.com/purview/sensitivity-labels>).
2. Microsoft Purview - "Create and configure sensitivity labels", section "Scope", bullets 1-2: Files & emails vs. Groups & sites (same page).
3. Microsoft Purview - "Publish sensitivity labels", section "Choose which users and groups get the labels" (<https://learn.microsoft.com/purview/publish-labels>).
4. Microsoft Purview - "Automatically apply or recommend a sensitivity label", note: "If 'Users can't apply this label...' is selected, the label isn't shown in apps" (<https://learn.microsoft.com/purview/sensitivity-labels-automatic>).

Question: 16

You have a Microsoft 365 subscription. All users have their email stored in Microsoft Exchange Online. In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX. What should you do first?

- A. From the Exchange admin center create a mail flow rule.
- B. From Microsoft 365 Defender, start a message trace.
- C. From Microsoft Defender for Cloud Apps, create an activity policy.
- D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer:

D

Explanation:

The requirement is to preserve a copy of specific emails for compliance or legal purposes. The correct tool for this within Microsoft 365 is Microsoft Purview. The first step is to create a retention label that defines the preservation settings. Subsequently, you would create an auto-apply label policy that uses a Keyword Query Language (KQL) query for "ProjectX" to automatically find and apply this label to all relevant emails in User1's mailbox. This ensures the items are preserved and cannot be permanently deleted by the user.

Why Incorrect Options are Wrong:

- A. A mail flow rule can copy messages in transit, but it does not preserve the original item in the user's mailbox if the user deletes it.
- B. A message trace is a diagnostic tool used to track the delivery status of emails after they have been sent; it does not preserve content.
- C. A Microsoft Defender for Cloud Apps activity policy is used for security monitoring and to trigger alerts or governance actions based on user activities, not for content preservation.

References:

1. Microsoft Learn. "Learn about retention policies & retention labels." Microsoft Purview documentation. This document states, "Use a retention label to... Retain content forever or for a specific period of time." It also clarifies that labels are applied to individual items like emails.
2. Microsoft Learn. "Automatically apply a retention label to retain or delete content." Microsoft Purview documentation. This guide details the process: "The conditions for auto-applying retention labels support keyword query language (KQL)... For example, you can configure a policy to automatically apply a retention label to all emails... that contain specific words." This directly maps to the scenario of preserving emails containing "ProjectX".

3. Microsoft Learn. "Mail flow rules (transport rules) in Exchange Online." Exchange Online documentation. This source explains that mail flow rules inspect messages in transit and take actions like redirecting or blocking, which is distinct from the compliance preservation required in the question.

CertEmpire

Question: 17

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune. You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

- A. Device1 only
- B. Device1 and Device4
- C. Device1, Device3, and Device4
- D. Device1, Device2, Device3, and Device4

Answer:

CertEmpire

A

Explanation:

Delivery Optimization is a peer-to-peer distribution technology designed specifically for Windows clients (Windows 10 and Windows 11) to share the burden of downloading updates and apps. Configuration profiles in Microsoft Intune that contain Delivery Optimization settings can only be applied to devices running a supported Windows operating system. Among the listed devices, only Device1 runs Windows 11 Enterprise, which is a supported platform. The other operating systems-iOS, Android, and macOS-do not support the native Windows Delivery Optimization feature and will ignore these specific settings.

Why Incorrect Options are Wrong:

- B. Device1 and Device4: Incorrect because macOS (Device4) does not support the Windows Delivery Optimization feature.
- C. Device1, Device3, and Device4: Incorrect because Android (Device3) and macOS (Device4) do not support Windows Delivery Optimization.
- D. Device1, Device2, Device3, and Device4: Incorrect because iOS (Device2), Android (Device3), and macOS (Device4) do not support Windows Delivery Optimization.

References:

1. Microsoft Learn. (2023). What is Delivery Optimization? Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization>.
Reference Details: The "In this article" section and the main body explicitly state, "Delivery Optimization is a peer-to-peer distribution technology in Windows 10 and Windows 11..." It lists the supported Windows editions, with no mention of other operating systems.
2. Microsoft Learn. (2024). Delivery Optimization settings in Microsoft Intune. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings>.
Reference Details: The "Applies to" section at the top of the document clearly specifies "Windows 10 and later," confirming that these Intune settings are exclusive to Windows devices.
3. Microsoft Learn. (2023). Delivery Optimization for Windows updates. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization>.
Reference Details: The "Requirements" section lists the supported Windows 10 and Windows 11 editions (Pro, Enterprise, Education), reinforcing that the feature is Windows-specific.

CertEmpire

Question: 18

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

- A. Policy1 and Policy2 only
- B. Policy2 and Policy4 only
- C. Policy3 and Policy4 only
- D. Policy1 and Policy3only

CertEmpire

Answer:

A

Explanation:

In Microsoft Defender for Office 365, quarantine policies define user capabilities for quarantined messages and the retention period. These customizable quarantine policies can be assigned to supported protection features. Specifically, both anti-spam and anti-phishing policies support the assignment of custom quarantine policies, which allows an administrator to define a specific retention period (from 1 to 30 days).

Conversely, messages quarantined by anti-malware and Safe Attachments policies are governed by a default, non-customizable system policy named AdminOnlyAccessPolicy. This policy has a fixed retention period and does not permit customization. Therefore, only anti-phishing (Policy1) and anti-spam (Policy2) support a customized quarantine retention period.

Why Incorrect Options are Wrong:

- B. Policy2 and Policy4 only: This is incorrect because anti-malware policies (Policy4) use a default, non-customizable quarantine policy with a fixed retention period.
- C. Policy3 and Policy4 only: This is incorrect because neither Safe Attachments (Policy3) nor anti-malware (Policy4) policies support the assignment of custom quarantine policies for retention.

D. Policy1 and Policy3 only: This is incorrect because Safe Attachments policies (Policy3) use a default, non-customizable quarantine policy with a fixed retention period.

References:

1. Microsoft Learn. (2024). Quarantine policies. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide>.

Reference Details: Under the section "Supported features in quarantine policies," the table explicitly lists "Anti-spam policy" and "Anti-phishing policy" as supporting quarantine policies. It also notes that for "Anti-malware policy" and "Safe Attachments policy," messages are quarantined by default with no option to assign a custom quarantine policy.

2. Microsoft Learn. (2024). Recommended settings for EOP and Microsoft Defender for Office 365 security. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide>.

Reference Details: In the tables for "Standard preset security policy settings" and "Strict preset security policy settings," the actions for Anti-phishing and Anti-spam verdicts show "Quarantine the message" and specify a quarantine policy. In contrast, the actions for Anti-malware and Safe Attachments simply state "Quarantine the message," indicating the use of the default, non-configurable policy.

3. Microsoft Learn. (2024). Manage quarantined messages and files as an admin in Microsoft 365. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide>.

Reference Details: The section "Quarantine retention" states, "By default, messages that were quarantined for spam, bulk, or phish are stored for 30 days... Messages quarantined by anti-malware policies... are stored for 30 days." It clarifies that the retention for spam, bulk, and phish is controlled by the "Retain spam in quarantine for this many days" setting in anti-spam policies, confirming its customizability, whereas malware retention is fixed.

Question: 19

You purchase a new computer that has Windows 10, version 21H1 preinstalled. You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed. What should you do on the computer?

- A. Install all the feature updates released since version 21H1 and the latest quality update only.
- B. Install the latest feature update and all the quality updates released since version 21H1.
- C. Install the latest feature update and the latest quality update only.
- D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer:

C

Explanation:

Windows 10 updates are designed to be cumulative to simplify the update process. A feature update (e.g., upgrading from version 21H1 to 22H2) is a complete operating system installation that includes all features from previous versions. Therefore, only the single latest feature update is required.

Similarly, quality updates (also known as Latest Cumulative Updates or LCUs) contain all the fixes from previous quality updates for that specific feature version. Installing only the latest quality update brings the device fully up-to-date with security and reliability patches. This two-step approach—installing one feature update and one quality update—is the most efficient method and minimizes the number of installations.

Why Incorrect Options are Wrong:

- A. Installing all feature updates is redundant. The latest feature update is inclusive of all preceding ones, making intermediate installations unnecessary and inefficient.
- B. Installing all quality updates is unnecessary. The latest quality update is cumulative and contains all the fixes from previous months for that specific feature version.
- D. This option is the least efficient. It combines the redundant installation of all intermediate feature updates with the unnecessary installation of all individual quality updates.

References:

1. Microsoft Learn. (2023). Overview of Windows as a service.

Section: Types of updates Quality updates.

Content: "Quality updates are cumulative, so installing the latest quality update is sufficient to get all the available fixes for a specific feature update." This confirms that only the latest quality update is needed.

2. Microsoft Learn. (2023). Windows client servicing terminology.

Section: Feature update.

Content: "Feature updates are released annually... Because they are cumulative, they include all previous fixes." This supports installing only the latest feature update to get all features and fixes up to that point.

3. Microsoft Learn. (2023). Windows Update for Business deployment service.

Section: About Windows updates Feature updates.

Content: "Feature updates for Windows 10 and Windows 11 are released annually... Since feature updates are cumulative, you only need to install the latest feature update to get all the new features and fixes." This explicitly states the principle of installing only the latest feature update.

Question: 20

You have a Microsoft 365 E5 tenant. You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected. What should you use to create the policy?

- A. the Microsoft 365 admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft Defender for Cloud Apps portal
- D. the Microsoft Apps admin center

Answer:

C

Explanation:

The requirement is to create a policy that alerts on unusual Microsoft Office 365 usage patterns. This capability is a core feature of User and Entity Behavior Analytics (UEBA) provided by a Cloud Access Security Broker (CASB). Microsoft Defender for Cloud Apps is the Microsoft 365 CASB solution, included in the E5 license. It uses machine learning to analyze user activities and create a baseline of normal behavior. The anomaly detection policies within the Defender for Cloud Apps portal are specifically designed to identify and trigger alerts for deviations from this baseline, such as impossible travel, mass downloads, or activity from suspicious IP addresses.

Why Incorrect Options are Wrong:

- A. The Microsoft 365 admin center is used for general tenant administration, such as managing users and licenses, not for creating advanced behavioral anomaly detection policies.
- B. The Microsoft Purview compliance portal is focused on data governance, information protection, and compliance policies (like DLP), not on detecting anomalous user behavior patterns.
- D. The Microsoft Apps admin center is used to manage Office app deployments, add-ins, and service settings, and lacks security monitoring or alerting capabilities.

References:

1. Microsoft Learn. (2023). Anomaly detection policies in Microsoft Defender for Cloud Apps. "Microsoft Defender for Cloud Apps anomaly detection policies provide out-of-the-box user and entity behavioral analytics (UEBA) and machine learning (ML) so that you can immediately run advanced threat detection across your cloud environment." This document details the types of policies available, such as "Impossible travel" and "Unusual multiple file download," which directly address the question's requirement. (Reference: <https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy>)

2. Microsoft Learn. (2023). What is Defender for Cloud Apps? "Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB)... provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services." (Reference:

<https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>, Introduction section)

3. Microsoft. (2023). Microsoft 365 guidance for security & compliance. This official licensing guide confirms that Microsoft Defender for Cloud Apps is included as a feature within the Microsoft 365 E5 license suite. (Reference: <https://learn.microsoft.com/en-us/office365/servicesdescriptions/microsoft-365-service-descriptions/microsoft-365-tenant-level-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance>, See the feature table for Microsoft 365 E5/A5/G5 Security)

CertEmpire

Question: 21

DRAG DROP You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices. You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of policy should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Policy Types	Answer Area
<input type="text" value="App configuration policy"/> <input type="text" value="App protection policy"/> <input type="text" value="Compliance policy"/> <input type="text" value="Conditional Access policy"/>	Device1: <input type="text"/> Device2: <input type="text"/> Device3: <input type="text"/>

Answer:

Device1: App protection policy

Device2: Conditional Access policy

Device3: App protection policy

Explanation:

Here is the reasoning for each policy assignment:

- Device1 (Windows 11): The requirement is to encrypt Word files. An App protection policy for Windows devices includes data protection settings, such as encrypting corporate data, which protects data at the application level.

- Device2 (iOS): The goal is to block native/third-party mail clients and force the use of an approved app (like Microsoft Outlook) to access Microsoft 365. A Conditional Access policy is used to enforce this by setting the "Grant" control to "Require approved client app." This blocks all non-approved applications from accessing the specified cloud resources (like Exchange Online).
- Device3 (Android): The requirement is to block access from Word if the device is jailbroken. Critically, this device is Not enrolled in Intune. An App protection policy can be applied to unenrolled devices (MAM-WE) and uses "Conditional launch" settings. These settings can check for device conditions, such as being "Jailbroken/rooted," and then block access to corporate data within the app.

References:

Microsoft Intune Documentation (App protection policy for Device3):

Source: Microsoft Learn, "App protection policy settings for Android"

Reference: In the "Conditional launch" section, "Device conditions" includes the setting Jailbroken/rooted devices. The available actions for this setting are Block access, Wipe data, or Warn. This directly maps to the requirement for Device3.

Location: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#conditional-launch>

CertEmpire

Microsoft Entra Documentation (Conditional Access for Device2):

Source: Microsoft Learn, "Conditional Access: Grant controls"

Reference: The "Require approved client app" grant control is used to force specific applications to be used for accessing cloud apps. The documentation states, "This control requires that a client app from an approved list is used to access the selected cloud apps... Examples of approved client apps include... Microsoft Outlook." This control effectively blocks native mail clients.

Location: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-approved-client-app>

Microsoft Intune Documentation (App protection policy for Device1):

Source: Microsoft Learn, "App protection policy settings for Windows"

Reference: The "Data protection" section for Windows APP settings lists a setting to Encrypt corporate data. This setting, when configured, ensures that corporate data within policy-managed apps (like Word) is encrypted on the device.

Location: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-windows#data-protection>

Question: 22

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site. What should you do?

- A. From the SharePoint Online site, create an alert.
- B. From the SharePoint Online admin center, modify the sharing settings.
- C. From the Microsoft 365 Defender portal, create an alert policy.
- D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

Answer:

D

Explanation:

A Microsoft Purview Data Loss Prevention (DLP) policy is the appropriate tool for this requirement. DLP policies can be scoped to specific locations, such as the human resources department's SharePoint Online site. You can configure a rule within the policy to detect when content is shared with people outside the organization. A key action for this rule is to send an email notification (an incident report) to a specified individual, such as the department manager, providing details of the sharing event. This provides a robust, policy-based monitoring and notification system specifically for data sharing activities.

Why Incorrect Options are Wrong:

A. From the SharePoint Online site, create an alert.

SharePoint alerts notify users of changes to content (add, modify, delete) but do not have a specific, reliable trigger for sharing events. They are not designed for policy-based monitoring.

B. From the SharePoint Online admin center, modify the sharing settings.

These settings control if and how users can share content (e.g., disabling anonymous links). They do not provide a mechanism to send notifications when a sharing event occurs.

C. From the Microsoft 365 Defender portal, create an alert policy.

While alert policies can be triggered by audit log events, including sharing, DLP is the more specific and purpose-built service for monitoring and controlling data sharing based on content and context.

References:

1. Microsoft Learn. "Learn about data loss prevention." Microsoft Purview Documentation. This document outlines the capabilities of DLP, stating, "A DLP policy allows you to... Show a policy tip to users who are about to share sensitive information... Send an email notification to your compliance officer when a user shares sensitive information." This confirms that sending

notifications based on sharing is a core DLP function.

2. Microsoft Learn. "Create and Deploy data loss prevention policies." Microsoft Purview Documentation. Under the "Policy settings" section, it details how to configure rules. For the "Actions" configuration, it lists "Send alerts to admins" and allows customization of who receives the alert and the email content, directly supporting the solution.

3. Microsoft Learn. "Create an alert to get notified when a file or folder changes in SharePoint." Microsoft Support Documentation. This article shows that the available triggers for SharePoint alerts are for when items are changed, added, or deleted, with no specific option for "when an item is shared."

CertEmpire

Question: 23

HOTSPOT You have a Microsoft 365 E5 subscription that. You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription. Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area. **NOTE** Each correct selection is worth one point.

Answer Area

Feature:

- Activity explorer
- Compliance Manager
- Content explorer

Number of days the data will be retained:

- 30
- 60
- 120

Answer:

Feature: Activity explorer

Number of days the data will be retained: 30 CertEmpire

Explanation:

Activity explorer is the correct feature because its specific function is to provide a visual interface for monitoring activities related to information protection, including sensitivity labels. It aggregates data from the unified audit log to show when a label was "applied, changed, or removed" and by whom.

- Compliance Manager is incorrect as it tracks an organization's overall compliance posture against regulations and standards, not specific file-level user activities.
- Content explorer is incorrect as it is used to view the contents of files that have been classified, not the activity logs of when the classifications occurred.

According to official Microsoft documentation, the Activity explorer interface surfaces data from the last 30 days. While the underlying Microsoft 365 E5 audit log retains this data for one year, the Activity explorer tool itself is limited to a 30-day visualization window.

References:

Microsoft. (2024, September 27). Get started with activity explorer. Microsoft Learn. Retrieved October 20, 2025.

Reference: This document states, "Activity explorer provides a historical view... of activities related to... sensitivity labels..." and "Activity explorer... activities are available in Activity explorer for 30 days."

Microsoft. (2024, September 27). Learn about content explorer. Microsoft Learn. Retrieved October 20, 2025.

Reference: This document confirms that Content explorer's function is to "view the items that were summarized in... data classification" to "review the content in its native format."

Microsoft. (2024, June 21). Learn about auditing solutions in Microsoft Purview. Microsoft Learn. Retrieved October 20, 2025.

Reference: This document clarifies that while Microsoft 365 E5 licenses include a "default retention of one year" for audit logs (the data source), this is distinct from the 30-day visualization window of the Activity explorer tool itself.

Question: 24

HOTSPOT You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune. You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users. Policy! has the Data protection settings shown in the following exhibit.

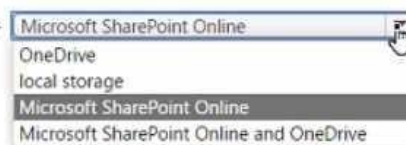
Data Transfer

Backup org data to Android backup services ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Send org data to other apps ⓘ	Policy managed apps
Select apps to exempt	<input type="button" value="Select"/>
Save copies of org data ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Allow user to save copies to selected services ⓘ	SharePoint
Transfer telecommunication data to ⓘ	Any dialer app
Dialer App Package ID	<input type="text"/>
Dialer App Name	<input type="text"/>
Receive data from other apps ⓘ	All Apps
Open data into Org documents ⓘ	<input type="radio"/> Allow <input type="radio"/> Block
Allow users to open data from selected services ⓘ	3 selected
Restrict cut, copy, and paste between other apps ⓘ	Policy managed apps with paste in
Screen capture and Google Assistant ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Approved keyboards ⓘ	<input type="radio"/> Require <input checked="" type="radio"/> Not required
Select keyboards to approve	<input type="button" value="Select"/>

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

A user can copy files from Microsoft OneDrive to [answer choice] only.



A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

**Answer:**

Statement 1: Microsoft SharePoint Online

Statement 2: any app

Explanation:

Save Copies: The policy setting "Save copies of org data" is set to "Block". This prevents users from saving organizational data to arbitrary locations, such as unmanaged local storage. However, the exception setting "Allow user to save copies to selected services" is explicitly configured to permit saving to "SharePoint". Therefore, SharePoint Online is the only configured allowable location.

CertEmpire

Copy/Paste: The policy setting "Receive data from other apps" is set to "All Apps". Furthermore, the setting "Restrict cut, copy, and paste between other apps" is set to "Policy managed apps with paste in". This specific value explicitly allows users to paste data from any app (managed or unmanaged) into policy-managed apps (like the Word document on OneDrive).

References:

Microsoft Learn. (n.d.). Android app protection policy settings in Microsoft Intune. Retrieved October 20, 2025.

Reference for Statement 1: In the "Data protection" section, under "Data Transfer," the documentation for the "Allow user to save copies to selected services" setting states: "When Save copies of org data is set to Block, you can allow end users to save copies of org data to a selected service, such as SharePoint."

Reference for Statement 2: In the same "Data Transfer" section, the documentation for "Restrict cut, copy, and paste between other apps" explains the value "Policy managed apps with paste in": "Allow cut or copy from any app and paste into policy-managed apps." The "Receive data from other apps" setting further confirms this, as "All apps" allows "data transfer from any app" into the managed app.

Question: 25

HOTSPOT You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You are implementing Microsoft Defender for Endpoint. You need to enable role-based access control (RBAC) to restrict access to the Microsoft 365 Defender portal. Which users can enable RBAC, and which users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area. **NOTE** Each correct selection is worth one point.

Answer Area

Users that can enable RBAC:

- Admin1 and Admin2 only
- Admin1 only
- Admin1 and Admin2 only
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

- Admin3, Admin4, and Admin5 only
- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only

Answer:

Users that can enable RBAC: Admin1 and Admin2 only

Users that will no longer have access to the Microsoft 365 Defender portal: Admin3 and Admin4 only

Explanation:

Users that can enable RBAC: To enable role-based access control (RBAC) within the Microsoft Defender for Endpoint settings, a user must hold either the Global Administrator (Admin1) or Security Administrator (Admin2) role in Azure Active Directory (Azure AD).

Users that will no longer have access: Before MDE RBAC is enabled, access to the portal is

governed by Azure AD roles, including Global Administrator, Security Administrator, Security Operator, and Security Reader. When MDE RBAC is turned on, users who only have Security Operator (Admin3) or Security Reader (Admin4) roles immediately lose their access. Global and Security Administrators (Admin1, Admin2) retain their access. The Application Administrator (Admin5) role does not grant access to the Defender portal, so Admin5 never had access to lose.

References:

Microsoft Learn. (2025, October 15). Manage portal access using role-based access control. "To turn on role-based access control (RBAC)... You need to have a Global Administrator or Security Administrator role in Azure AD." (Retrieved from the "Turn on role-based access control" section).

Microsoft Learn. (2025, October 15). Manage portal access using role-based access control. "When you turn on role-based access control, users with only Global Administrator or Security Administrator roles in Azure AD retain access to the portal with full permissions... Other roles in Azure AD (such as Security Operator or Security Reader) lose access to the portal..." (Retrieved from the "Turn on role-based access control" section).

Microsoft Learn. (2025, October 11). Permissions in the Microsoft 365 Defender portal. This document details the permissions granted by Azure AD built-in roles, confirming that Application Administrator is not a role that provides default access to Microsoft Defender for Endpoint data. (Retrieved from the "Azure AD built-in roles" section).

CertEmpire

Question: 26

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps. You need to be notified when a single user downloads more than 50 files during any 60-second period.

What should you configure?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an anomaly detection policy

Answer:

C

Explanation:

An activity policy is the correct tool to create an alert for a specific, user-defined threshold of repeated actions within a set timeframe. The requirement is to be notified when a single user downloads more than 50 files in 60 seconds. This can be configured precisely using an activity policy by setting the activity type to "File downloaded" and using the "Repeated activity" parameter to specify the count (50) and the time period (60 seconds). This policy type provides the exact control needed to meet the specified conditions.

Why Incorrect Options are Wrong:

- A. a session policy: Session policies are used for real-time monitoring and control of user sessions (e.g., blocking downloads from unmanaged devices), not for generating alerts based on the rate of activity.
- B. a file policy: File policies are designed to scan and apply controls to files at rest within connected cloud applications (e.g., finding publicly shared sensitive files), not to monitor real-time user activities.
- D. an anomaly detection policy: Anomaly detection policies alert on deviations from a learned behavioral baseline. While there is a "Mass download" policy, it triggers when a user's activity is unusual compared to their baseline, not based on a fixed, predefined threshold like "50 files in 60 seconds".

References:

1. Microsoft Learn. (2024). Activity policies in Microsoft Defender for Cloud Apps. This document explicitly states that activity policies can be used to "Trigger an alert when a user performs the same activity a defined number of times in a defined timeframe." This directly maps to the question's requirement. (Section: "Create an activity policy").
2. Microsoft Learn. (2024). Anomaly detection policies in Microsoft Defender for Cloud Apps. This

source describes the "Mass download by a single user" policy, clarifying that it "identifies a user that downloads an unusually high number of files compared to the learned baseline." This confirms it is for behavioral anomalies, not fixed thresholds. (Section: "Mass download by a single user").

3. Microsoft Learn. (2024). Session policies. This document details how session policies provide "granular visibility into cloud apps and the ability to control different actions within a session in real time," which is distinct from rate-based alerting. (Section: "What are session policies?").

4. Microsoft Learn. (2024). File policies. This source explains that file policies are used to "scan for specific files that may put you at risk," focusing on files at rest rather than user actions. (Section: "What are file policies?").

Question: 27

HOTSPOT You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

No

No

No

Explanation:

This scenario depends on two factors: Role Permissions (what a user can do) and Device Group Access (what devices a user can act on). A user must have both the correct permission and access to the device group.

- User1 can run an antivirus scan on Device2. (No)
- Permission: User1 is in Group1, which has Role1. Role1 grants "View data" and "Alerts investigation." Running an antivirus scan is an "Active remediation action," which Role1 does not have.
- Access: Device2 is in the "Ungrouped devices" group, which is scoped for access by Group2. User1 is in Group1.
CertEmpire
- Conclusion: User1 fails on both permission and access.
- User2 can collect an investigation package from Device2. (No)
- Access: User2 is in Group2, and Device2's group is scoped to Group2. User2 does have access to the device.
- Permission: User2 is in Group2, which has Role2. Role2 only grants "View data." Collecting an investigation package requires "Alerts investigation" or "Active remediation actions" permission.
- Conclusion: User2 has access but lacks the necessary permission.
- User3 can isolate Device1. (No)
- Permission: User3 is in Group3, which has the "Microsoft Defender for Endpoint administrator" role. This role does include "Active remediation actions," which is required to isolate a device.
- Access: Device1 is in the "ATP1" device group, which is scoped for access by Group1. User3 is

in Group3.

- Conclusion: User3 has the permission but lacks access to the device group containing Device1.

References:

Microsoft Defender for Endpoint Documentation (learn.microsoft.com). Create and manage roles for role-based access control.

Relevance: This document details the built-in roles and their specific permissions. It confirms that actions like running an AV scan or isolating a device fall under "Active remediation actions." It also confirms that collecting an investigation package is part of "Alerts investigation" or "Active remediation actions," both of which are beyond "View data."

Microsoft Defender for Endpoint Documentation (learn.microsoft.com). Create and manage device groups in Microsoft Defender for Endpoint.

Relevance: This document explains that to perform actions on devices, a user must be part of a user group (like Group1, Group2, or Group3) that is explicitly granted "User access" to the corresponding device group (like ATP1 or Ungrouped devices). This confirms the access scoping logic used in the explanation.

Question: 28

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2. The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2. You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1. You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers. Does this meet the goal?

- A. Yes
- B. No

Answer:

CertEmpire

- B

Explanation:

The solution fails because it specifies copying the Administrative Templates (ADMX/ADML files) to the incorrect location. To make new Group Policy settings available for domain-wide management, a Central Store must be created in the SYSVOL share (\\SYSVOL\\Policies\\PolicyDefinitions), not the Netlogon share. The Group Policy Management Console (GPMC) does not load templates from the Netlogon share. Additionally, raising the domain functional level is not required to manage client-side Group Policy settings; the availability of settings is determined by the ADMX templates loaded by the GPMC, not the domain's functional level.

Why Incorrect Options are Wrong:

A. Yes: This is incorrect because the proposed steps will not make the Windows 10 WUfB settings available in the GPMC, as the templates are copied to the wrong location.

References:

1. Microsoft Learn. (2023, October 12). Create and manage the Central Store for Group Policy Administrative Templates in Windows. "To take advantage of the benefits of .admx files, you must create a Central Store in the SYSVOL folder on a Windows domain controller... The Group Policy tools use only the .admx files that are in the Central Store. The tools ignore any .admx files that are stored in the local PolicyDefinitions folder... The path is \\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions."
2. Microsoft Learn. (2023, September 21). Active Directory Domain Services Functional Levels in Windows Server. This document details the features enabled by different functional levels. None of these features are related to the management of Group Policy settings from specific Administrative Templates. This confirms that raising the functional level is an unnecessary step for the stated goal.

CertEmpire

Question: 29

Your company has a Microsoft 365 subscription. You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license. What should you use?

- A. Active users in the Microsoft 365 admin center
- B. Reports in Microsoft Purview compliance portal
- C. the Licenses blade in the Microsoft Entra admin center
- D. Reports in the Microsoft 365 admin center

Answer:

C

Explanation:

The Microsoft Entra admin center is the designated portal for managing and viewing group-based licensing assignments. Within the Licenses blade (Identity Billing Licenses), an administrator can select a specific product license (e.g., Office 365 E3). This view provides a list of all groups that are assigned that license. By selecting a group from this list, you can then view its members, thereby identifying all users who are licensed through that specific group. This method directly and efficiently addresses both requirements of the question: identifying the users and the group that provides the license.

Why Incorrect Options are Wrong:

A. Active users in the Microsoft 365 admin center

This view can show if a user has a license, but it does not provide an efficient way to filter or report on all users based on the group assignment method.

B. Reports in Microsoft Purview compliance portal

The Microsoft Purview compliance portal is used for data governance, risk management, and compliance, not for license management or reporting on license assignments.

D. Reports in the Microsoft 365 admin center

The reports in this section focus on service usage, user activity, and adoption metrics, not on the administrative details of how licenses were assigned (e.g., direct vs. group-based).

References:

1. Microsoft Entra ID Documentation, "Assign licenses to users by group membership in Microsoft Entra ID." Microsoft Learn. This document outlines the procedure for group-based licensing. It specifies the navigation path: "Sign in to the Microsoft Entra admin center... Browse to Identity Billing Licenses." It then details how to select a product and view the groups to which it is

assigned.

2. Microsoft Entra ID Documentation, "What is group-based licensing in Microsoft Entra ID?" Microsoft Learn. This foundational document explains that group-based licensing is managed within Microsoft Entra ID, establishing the Entra admin center as the correct location for this task.

3. Microsoft 365 Documentation, "Microsoft 365 Reports in the admin center." Microsoft Learn. This source details the available reports in the Microsoft 365 admin center. A review of the reports, such as "Active users" or product usage reports, confirms they show license status and usage but do not detail the assignment source (direct vs. group).

CertEmpire

Question: 30

HOTSPOT You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support. How should you complete the membership rule? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

(user.userType

- eq "Guest"
- in "Guest"
- ne "Guest"
- notmatch "Member"

- contains "Support"
- in "Support"
- match "Support"
- startsWith "Sup"

Answer:

Box 1: (user.userType -eq "Guest") and (user.department

Box 2:) and (user.department -contains "Support")

Explanation:

To configure the dynamic membership rule, two conditions must be met, joined by the -and operator.

- Guest User Selection: The first part of the rule must identify users who are guests. The user.userType attribute holds this information. The -eq (equals) operator provides a precise match for the string value "Guest".
- Department Selection: The second part must find users whose department attribute contains the word "Support". The -contains operator is used for partial string matches, which will correctly find "Support" within values like "IT support" and "SupportCore".

The operator `-in` is incorrect as it is used to check if a property matches any value in a collection (e.g., `user.department -in "Sales", "Finance"`), not for partial string matching.

References:

Microsoft Entra ID Documentation (Official Vendor). "Dynamic membership rules for groups in Microsoft Entra ID." Microsoft Learn.

Reference (Box 1): In the section "Rule for guests," Microsoft provides the exact syntax for finding guest users: `(user.userType -eq "Guest")`. This confirms `-eq` is the correct operator for matching the "Guest" user type.

Reference (Box 2): In the section "Supported expression rule operators," the `-contains` operator is defined as "String contains. Performs partial string matches." This is the correct operator for finding "Support" as a substring within the `user.department` attribute.

Reference (Incorrect Options): The same document clarifies that the `-in` operator is used to "Match against a collection of constants" (e.g., an array of strings), which is not the requirement for either condition.

Question: 31

HOTSPOT Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription. You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center. Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.

Answer Area

File type to use:

▼
CSV
JSON
PST
XML

Required properties for each user:

▼
Display Name and Department
First Name and Last Name
User Name and Department
User Name and Display Name

Answer:

File type to use: CSV

Required properties for each user: User Name and Display Name

Explanation:

The Microsoft 365 admin center's "Add multiple users" wizard is designed to import users in bulk using a Comma Separated Values (CSV) file.

According to the official Microsoft 365 documentation for this procedure, the CSV file template has several available columns, but only two are mandatory for the import to function:

- **User Name:** This field is used for the User Principal Name (UPN), which is the user's sign-in ID (e.g., user@company.com).
- **Display Name:** This is the friendly name that appears for the user in the address book and other Microsoft 365 services.

All other properties, such as First Name, Last Name, and Department, are optional.

References:

Microsoft Learn. (2024, September 27). Add several users at the same time to Microsoft 365 - Microsoft 365 admin.

Page/Section: In the "Import multiple users" panel description and the "Fill out the CSV file" section.

Quote/Paraphrase: The documentation states, "On the Import multiple users panel, you can optionally download a sample CSV file... The required column headers are User Name and Display Name."

Microsoft Learn. (2024, June 12). Bulk create users in the Microsoft Entra admin center. (Microsoft Entra ID is the underlying identity service for Microsoft 365).

Page/Section: "Understand the CSV template" section.

Quote/Paraphrase: The documentation for the corresponding bulk-create template in Microsoft Entra (Azure AD) confirms this requirement. The template properties list "User principal name userPrincipalName Required." and "Name displayName Required." "User principal name" corresponds to "User Name," and "Name" corresponds to "Display Name."

CertEmpire

Question: 32

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements: To all users, deploy an Office 365 E3 license without the Power Automate license option. To all users, deploy an Enterprise Mobility + Security E5 license. To the users in the research department only, deploy a Power BI Pro license. To the users in the marketing department only, deploy a Visio Plan 2 license. What is the minimum number of deployment groups required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

CertEmpire

Answer:

C

Explanation:

The licensing requirements can be met by creating three distinct groups based on the user populations and their specific license needs.

1. Group 1 (All Users): This group will contain all users (User1, User2, User3, User4, User5). It will be assigned the Office 365 E3 license (with the Power Automate service plan disabled) and the Enterprise Mobility + Security E5 license. This fulfills the two requirements applicable to everyone.

2. Group 2 (Research Department): This group will contain only the research users (User1, User3, User5). It will be assigned the Power BI Pro license.

3. Group 3 (Marketing Department): This group will contain only the marketing users (User2, User4). It will be assigned the Visio Plan 2 license.

This three-group structure correctly assigns all required licenses and logically separates the

common "base" licenses from the department-specific "add-on" licenses, representing the most efficient and scalable management approach.

Why Incorrect Options are Wrong:

- A. 1: A single group cannot be used, as it's impossible to selectively assign the Power BI Pro and Visio licenses to only specific members within that one group.
- B. 2: Using only two groups (e.g., one for Research and one for Marketing) would require assigning the common licenses (O365 E3 and EMS E5) to both groups, creating redundant management.
- D. 4: Four groups are unnecessary. The two licenses required by all users (Office 365 E3 and EMS E5) can be efficiently assigned to a single "all users" group.
- E. 5: Five groups are excessive. There are only three distinct licensing policies required for the specified user populations (All Users, Research, and Marketing).

References:

1. Microsoft Entra documentation, "What is group-based licensing in Microsoft Entra ID?": This document outlines the core principles. It states, "You can assign one or more license products to a group." This supports assigning both Office 365 E3 and EMS E5 to a single "All Users" group. It also explains that a user who is a member of multiple groups inherits the union of all assigned licenses, which is the principle that makes the three-group solution work. (See the section "How does group-based licensing work?").
2. Microsoft Entra documentation, "Assign licenses to users by group membership in Microsoft Entra ID": This guide provides scenarios for license management. The examples illustrate the best practice of using a base group for common licenses and then layering additional licenses for specific user sets via other groups, which directly supports the three-group answer. (See the section "Group-based licensing scenarios").
3. Microsoft Entra documentation, "Group-based licensing additional scenarios": This document details more complex situations, including how the system resolves license conflicts when a user is in multiple groups. The principle of license inheritance (union of services) is foundational to the solution requiring separate groups for separate license assignments. (See the section "Use multiple groups to manage licenses").

Question: 33

You have a Microsoft 365 subscription. You view the Service health Overview as shown in the following exhibit. You need to ensure that a user named User1 can view the advisories to investigate service health issues. Which role should you assign to User1?

- A. Message Center Reader
- B. Reports Reader
- C. Service Support Administrator
- D. Compliance Administrator

Answer:

C

Explanation:

The Service Support Administrator role is the most appropriate choice. This role is specifically designed for users who handle support-related tasks. It grants permissions to view the Service health dashboard and the Message Center, which are essential for investigating service issues. Additionally, this role allows the user to open and manage service requests with Microsoft, a common next step after an initial investigation. While other roles might have viewing permissions, the Service Support Administrator role's purpose directly aligns with the described task of investigating service health.

Why Incorrect Options are Wrong:

- A. Message Center Reader: While this role can view the Service health dashboard, its primary purpose is to read announcements about planned changes. The Service Support Administrator is a more suitable role for actively investigating service issues.
- B. Reports Reader: This role is incorrect. It only grants permissions to view usage reports (e.g., app usage, user activity) and does not provide access to the Service health dashboard.
- D. Compliance Administrator: This role is incorrect. It is focused on managing compliance features like eDiscovery and data loss prevention and has no permissions related to viewing service health.

References:

1. Microsoft Learn. (n.d.). About admin roles in the Microsoft 365 admin center.
Section: "Service support admin"
Content: "Can open support requests with Microsoft, and views the service dashboard and message center." This confirms that the role has the necessary viewing permissions for the task.
Section: "Reports reader"
Content: "Can view usage data and the reports dashboard in Microsoft 365 admin center..." This

confirms the role lacks permission for service health.

Section: "Message center reader"

Content: "Can read service notifications and health status in the Message center and on the Service health dashboard." This shows the role has technical permission but is less functionally aligned than the Service Support Administrator for an investigative task.

2. Microsoft Learn. (n.d.). How to check Microsoft 365 service health.

Section: "How to check service health"

Content: "To view service health, you must be a global administrator or a service support admin." (Note: The documentation sometimes provides a simplified list; the "About admin roles" page is more comprehensive, but this reference highlights Service Support Admin as a primary role for this function). This directly links the Service Support Administrator role to the action of checking service health.

Question: 34

HOTSPOT You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role: Scope type: Directory Selected members: Group1 Assignment type: Active Assignment starts: Mar 15, 2023 Assignment ends: Aug 15, 2023 You add the following assignment for the Exchange Administrator role: Scope type: Directory Selected members: Group2 Assignment type: Eligible Assignment starts: Jun 15, 2023 Assignment ends: Oct 15, 2023 For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements

On July 15, 2023, Admin1 can reset the password of a user.

Yes

No

On June 20, 2023, Admin2 can manage Microsoft Exchange Online.

On May 1, 2023, Admin3 can reset the password of a user.

Answer:

Yes

No

Yes

Explanation:

Statement 1 (Yes): The User Administrator role, which can reset passwords, is assigned to Group1. Admin1 is a member of Group1. The assignment is Active from March 15, 2023, to August 15, 2023. Since July 15, 2023, falls within this active period, Admin1 has the permissions.

Statement 2 (No): The Exchange Administrator role is assigned to Group2. Admin2 is a member

of Group2, and the date June 20, 2023, is within the assignment window. However, the assignment type is Eligible, not Active. This means Admin2 must first go through the Privileged Identity Management (PIM) process to activate the role. Without activation, the user does not have the permissions.

Statement 3 (Yes): The User Administrator role is assigned to Group1. Admin3 is a member of Group1. The assignment is Active from March 15, 2023, to August 15, 2023. Since May 1, 2023, falls within this active period, Admin3 has the permissions.

References:

Microsoft Entra documentation. (n.d.). Assign Microsoft Entra roles in Privileged Identity Management. Microsoft Learn. Retrieved October 20, 2025.

Reference: Section "Assign a role"

Quote: "There are two types of role assignments... Eligible assignments require the user to perform an action to use the role... Active assignments don't require the user to perform any action to use the role. Users assigned as active have the privileges assigned to the role."

Microsoft Entra documentation. (n.d.). Microsoft Entra built-in roles: User Administrator. Microsoft Learn. Retrieved October 20, 2025.

Reference: "User Administrator" role description table.

Quote: "Users with this role can... reset passwords... for all users and some administrators."

CertEmpire

Question: 35

You have a Microsoft 365 subscription. You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

Technical contact

User1@contoso.com ✓

Global privacy contact

✓

Privacy statement URL

http://contoso.com/privacy ✓

Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

Answer:

B

Explanation:

In Azure AD Tenant properties, the Privacy contact is the single address Microsoft uses for any personal-data or security-incident communications required under GDPR, including data-breach notices. The Technical contact, Marketing contact, or any other user accounts are not used for breach notification. In the exhibit, User2 is entered as the Privacy contact, while User3 is entered as the Technical contact; User1 is not listed at all. Therefore, only User2 will be contacted by Microsoft if the tenant is affected by a data breach.

Why Incorrect Options are Wrong:

- A. User1 is not configured as Privacy contact; Microsoft will not notify this user about breaches.
- C. User3 is listed as Technical contact only; technical contacts do not receive data-breach notices.
- D. User1 lacks any contact role and User2 alone meets the privacy-contact requirement.
- E. User3 (technical) is excluded from breach notifications; only User2 qualifies.

References:

1. Microsoft Docs - "Manage your Azure AD organization's privacy and contact info", section "Privacy contact" (para. 2) and "Notifications for personal data breaches" (<https://learn.microsoft.com/azure/active-directory/fundamentals/active-directory-tenant-properties>).
2. Microsoft 365 Compliance Center documentation - "How Microsoft provides data-breach notifications" (GDPR guidance), see "Customer privacy contacts" section (2023-05-18 version).
3. University of Washington, INFOSEC 542 course notes - "GDPR Articles 33-34 and cloud provider obligations", slide 15 (cites reliance on designated privacy contact for breach notice).