



# MS-102<sup>Q&As</sup>

Microsoft 365 Certified: Enterprise Administrator Expert

**Pass Microsoft MS-102 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/ms-102.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

You need to create the DLP policy to meet the technical requirements. What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlppolicy?view=o365-worldwide>

---

### QUESTION 2

#### HOTSPOT

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

Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Users who can assign Retention1:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

Users who can assign Retention2:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

Correct Answer:

Users who can assign Retention1:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

Users who can assign Retention2:

	▼
User4 only	
User3 and User4 only	
User2, User3, and User4 only	
User1, User2, User3, and User4	

**QUESTION 3**

**HOTSPOT**

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



Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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

Hot Area:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

**QUESTION 4**

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

Correct Answer: C

One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?



With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines

on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

<https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more>

### QUESTION 5

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

Correct Answer: A

### QUESTION 6

You have a Microsoft 365 subscription.

You suspect that several Microsoft Office 365 applications or services were recently updated.

You need to identify which applications or services were recently updated.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.



- A. From the Microsoft 365 admin center review the Service health blade
- B. From the Microsoft 365 admin center, review the Message center blade.
- C. From the Microsoft 365 admin center review the Products blade.
- D. From the Microsoft 365 Admin mobile app, review the messages.

Correct Answer: BD

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed

features, planned maintenance, or other important announcements.

The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.

Reference:

<https://docs.microsoft.com/en-us/office365/admin/manage/message-center>

<https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app>

## QUESTION 7

You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

- A. 20 hours
- B. 12 hours
- C. 7 hours
- D. 48 hours

Correct Answer: B



**QUESTION 8**

**HOTSPOT**

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

Name: Case1 Included content: Group1, User1, Site1 Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders

The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Holds are turned off for:

<input type="checkbox"/>	User1 only
<input type="checkbox"/>	All locations
<input type="checkbox"/>	Site1 and Group1 only

Holds are placed on a delay hold for:

<input type="checkbox"/>	30 days
<input type="checkbox"/>	90 days
<input type="checkbox"/>	120 days

Correct Answer:





Holds are turned off for:

	▼
User1 only	
All locations	
Site1 and Group1 only	

Holds are placed on a delay hold for:

	▼
30 days	
90 days	
120 days	

#### QUESTION 9

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records.

You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

- A. Configure custom detection rules.
- B. Create an Exact Data Match (EDM) schema.
- C. Run the Sec-RegulatoryComplianceUI cmdlet.
- D. Run the Sec-LabelPolicy cmdlet.

Correct Answer: C

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>

#### QUESTION 10

HOTSPOT

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

You plan to perform the following device management tasks in Microsoft Endpoint Manager:



Deploy a VPN connection by using a VPN device configuration profile. Configure security settings by using an Endpoint Protection device configuration profile.

You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

VPN device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Endpoint Protection device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Correct Answer:

VPN device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Endpoint Protection device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

### QUESTION 11

#### HOTSPOT

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.



You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Devices that can onboarded to Microsoft Defender for Endpoint:

<input type="checkbox"/>	Device 1 only
<input type="checkbox"/>	Device 1 and Device 2 only
<input type="checkbox"/>	Device 1 and Device 3 only
<input type="checkbox"/>	Device 1 and Device 4 only
<input type="checkbox"/>	Device 1, Device 2, and Device 4 only
<input type="checkbox"/>	Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

<input type="checkbox"/>	A conditional access policy only
<input type="checkbox"/>	A device compliance policy only
<input type="checkbox"/>	A device configuration profile only
<input type="checkbox"/>	A device configuration profile and a conditional access policy only
<input type="checkbox"/>	Device configuration profile, device compliance policy, and conditional access policy

Correct Answer:



Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

### QUESTION 12

DRAG DROP

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



**Actions**

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

**Answer Area**



Correct Answer:

**Actions**

Create an app configuration policy

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

**Answer Area**

Create a Google account

Link the account to Intune

Add the app

Assign the app



**QUESTION 13**



HOTSPOT

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen.

Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

ASR1:	<div style="border: 1px solid gray; padding: 2px; text-align: right;">▼</div>
	Device control
	Exploit protection
	Application control
	App and browser isolation
	Attack surface reduction rules
ASR2:	<div style="border: 1px solid gray; padding: 2px; text-align: right;">▼</div>
	Device control
	Exploit protection
	Application control
	App and browser isolation
	Attack surface reduction rules

Correct Answer:



ASR1:

	▼
Device control	
Exploit protection	
Application control	
App and browser isolation	
Attack surface reduction rules	

ASR2:

	▼
Device control	
Exploit protection	
Application control	
App and browser isolation	
Attack surface reduction rules	

**QUESTION 14**

**HOTSPOT**

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



### Answer Area

Tool:

AccessChk
Azure AD Connect
Active Directory Explorer
IdFix

Required group membership:

Domain Admins
Domain Users
Server Operators
Enterprise Admins

Correct Answer:

### Answer Area

Tool:

AccessChk
Azure AD Connect
Active Directory Explorer
IdFix

Required group membership:

Domain Admins
Domain Users
Server Operators
Enterprise Admins





### QUESTION 15

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.

Correct Answer: D

[MS-102 VCE Dumps](#)

[MS-102 Practice Test](#)

[MS-102 Study Guide](#)