

- **Vendor: Microsoft**
- **Exam Code: MS-101**
- **Exam Name: Microsoft 365 Mobility and Security**
- **New Updated Questions from [Braindump2go](#)**
- **(Updated in [November/2021](#))**

### **Visit Braindump2go and Download Full Version MS-101 Exam Dumps**

#### **QUESTION 364**

You have a Microsoft 365 tenant.  
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.  
What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

#### **QUESTION 365**

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

- A. Android Enterprise
- B. Windows 10
- C. Windows 8.1
- D. Android

**Answer: B**

**Explanation:**

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure>

#### **QUESTION 366**

You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.  
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.  
Which policy type should you configure?

- A. conditional access
- B. account protection

**[MS-101 Exam Dumps](#) [MS-101 Exam Questions](#) [MS-101 PDF Dumps](#) [MS-101 VCE Dumps](#)**

**<https://www.braindump2go.com/ms-101.html>**

- C. attack surface reduction (ASR)
- D. Endpoint detection and response

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

**QUESTION 367**

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.  
Which policy settings will be applied to Device1?

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

**Answer:** C

**QUESTION 368**

You have a Microsoft 365 E5 tenant that contains a user named User1.

You plan to implement insider risk management.

You need to ensure that User1 can perform the following tasks:

- Review alerts.
- Manage cases.
- Create notice templates.
- Review user emails by using Content explorer.

The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Insider Risk Management
- B. Insider Risk Management Analysts
- C. Insider Risk Management Investigators
- D. Insider Risk Management Admin

**Answer:** C

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide>

**QUESTION 369**

Your company has a Microsoft 365 E5 tenant that contains a user named User1.

You review the company's compliance score.

You need to assign the following improvement action to User1: Enable self-service password reset.

What should you do first?

[MS-101 Exam Dumps](#) [MS-101 Exam Questions](#) [MS-101 PDF Dumps](#) [MS-101 VCE Dumps](#)

<https://www.braindump2go.com/ms-101.html>

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

#### **QUESTION 370**

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard.

You need to assess the company's current state of compliance.

What should you use?

- A. eDiscovery
- B. Information governance
- C. Compliance Manager
- D. Data Subject Requests (DSRs)

**Answer: C**

**Explanation:**

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

#### **QUESTION 371**

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

- Microsoft Teams
- Microsoft OneDrive
- Microsoft Exchange Online
- Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

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

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide>

#### **QUESTION 372**

You have a Microsoft 365 E5 tenant.

You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.

You need to export the existing template.

Which file format should you use for the exported template?

- A. CSV
- B. XLSX
- C. JSON
- D. XML

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template>

**QUESTION 373**

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune. Company policy requires that the devices have the following configurations:

- Require complex passwords.
- Require the encryption of removable data storage devices.
- Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements.

What should you use?

- A. an app configuration policy
- B. a compliance policy
- C. a security baseline profile
- D. a conditional access policy

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

**QUESTION 374**

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

**Review your settings**

**Name**

Retention1

Edit

**Description for admins**

Edit

**Description for users**

Edit

**File plan descriptors**

Edit

Reference Id:1

Business function/department Legal

Category: Compliance

Authority type: Legal

**Retention**

Edit

7 years

Retain only

Based on when it was created

Back

Create this label

Cancel

When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.  
 What should you do?

- A. Create a new label policy
- B. Modify the Authority type setting for Retention1.
- C. Modify the Business function/department setting for Retention1.
- D. Use a file plan CSV template to import Retention1.

**Answer: A**

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>

**QUESTION 375**

You have the 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?

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

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

**QUESTION 376**

Hotspot Question

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

**[MS-101 Exam Dumps](#) [MS-101 Exam Questions](#) [MS-101 PDF Dumps](#) [MS-101 VCE Dumps](#)**


**<https://www.braindump2go.com/ms-101.html>**



Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.


The Products & services settings in Microsoft Store for Business are shown in the following exhibit.


**Microsoft Remote Desktop**  
 Free • Online • [Product Details](#)
Install

**Licenses**  
**Unlimited licenses**  
 0 used

**Billing**  
**€0.00** (Free app)

**Settings & Actions**  
 Not in private store  
[More actions available on details page](#)


**Excel Mobile**  
 Free • Online • [Product Details](#)
Install

**Licenses**  
**Unlimited licenses**  
 0 used

**Billing**  
**€0.00** (Free app)

**Settings & Actions**  
 In private store  
[More actions available on details page](#)

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
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

[MS-101 Exam Dumps](#) [MS-101 Exam Questions](#) [MS-101 PDF Dumps](#) [MS-101 VCE Dumps](#)

<https://www.braindump2go.com/ms-101.html>

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business>

**QUESTION 377**

Drag and Drop Question

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.

Which three 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.

**Actions**

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

**Answer Area**

Answer:

**Actions**

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

**Answer Area**

**Explanation:**

<https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security>

**QUESTION 378**

[MS-101 Exam Dumps](#) [MS-101 Exam Questions](#) [MS-101 PDF Dumps](#) [MS-101 VCE Dumps](#)

<https://www.braindump2go.com/ms-101.html>

**Hotspot Question**

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.

Home / Policy Management		Notifications
<b>Policy configurations</b>		
<a href="#">+ Create</a> <a href="#">Copy</a> <a href="#">Reorder priority</a> <a href="#">Remove</a>		Total policy configurations: 3
Name	Priority ↑	Recommendation status
<a href="#">Office Users Policy</a>	0	
<a href="#">Sales Team Policy</a>	1	
<a href="#">All users</a>	2	

The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

The default shared folder location for User1 is:

▼

[https://sharepoint.contoso.com/addins\\_all\\_users](#)  
[https://sharepoint.contoso.com/addins\\_office\\_users](#)  
[https://sharepoint.contoso.com/addins\\_sales\\_team\\_users\\_](#)

The default Office theme for User 2 is:

▼

[Colorful](#)  
[Dark Gray](#)  
[White](#)

**Answer:**



### Answer Area

The default shared folder location for User1 is:

▼

[https://sharepoint.contoso.com/addins\\_all\\_users](https://sharepoint.contoso.com/addins_all_users)  
[https://sharepoint.contoso.com/addins\\_office\\_users](https://sharepoint.contoso.com/addins_office_users)  
[https://sharepoint.contoso.com/addins\\_sales\\_team\\_users\\_](https://sharepoint.contoso.com/addins_sales_team_users_)

The default Office theme for User 2 is:

▼

[Colorful](#)  
[Dark Gray](#)  
[White](#)

#### Explanation:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

#### QUESTION 379

Hotspot Question

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

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input checked="" type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation:**

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

**QUESTION 380**

Hotspot Question

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.

**Answer Area**

Devices that can onboard 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

**Answer:**

**Answer Area**

Devices that can onboard 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

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view=o365-worldwide>

**QUESTION 381**

Hotspot Question

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

## Review your settings and finish

### Name

Sensitivity1

### Display name

Sensitivity1

### Description for users

Sensitivity1

### Scope

File.Email

### Encryption

### Content marking

Watermark: Watermark

Header: Header

### Auto-labeling

### Group settings

### Site settings

### Auto-labeling for database columns

None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

## Auto-labeling policy

[Edit Policy](#)[Delete Policy](#)**Policy name**

Auto-labeling policy

**Description****Label in simulation**

Sensitivity1

**Info to label**

IP Address

**Apply to content in these locations**

Exchange email All

**Rules for auto-applying this label**

Exchange email 1 rule

**Mode**

On

**Comment**

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	<b>Not applicable</b>	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

**QUESTION 382**

Hotspot Question

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

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

- Can be added to Compliance1 as recipients of noncompliance notifications
- Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Can be added to Compliance1 as recipients of noncompliance notifications:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Can be assigned to Compliance1:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

**Answer:**

### Answer Area

Can be added to Compliance1 as recipients of noncompliance notifications:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Can be assigned to Compliance1:

	▼
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group2 and Group3 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

**Explanation:**

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/>

**QUESTION 383**

Hotspot Question

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

**Compliance settings** [Edit](#)**Microsoft Defender ATP**

Require the device to be at or under the machine risk score: **Low**

**Device Health**

Rooted devices **Block**  
Require the device to be at or under the Device Threat Level

**System Security**

Require a password to unlock mobile devices **Require**  
Required password type **Device default**  
Encryption of data storage on device. **Require**  
Block apps from unknown sources **Block**

**Actions for noncompliance** [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

NOTE: Each correct selection is worth one point.

**Answer Area**

When a device reports a medium threat level, the device will

	▼
be locked remotely	
display a notification	
marked as compliant	
marked as noncompliant	
removed from the database	

Rooted devices will be

	▼
allowed to access company resources	
marked as compliant	
prevented from accessing company resources	
reported with a low device threat	

**Answer:**

**Answer Area**

When a device reports a medium threat level, the device will

	▼
be locked remotely	
display a notification	
marked as compliant	
marked as noncompliant	
removed from the database	

Rooted devices will be

	▼
allowed to access company resources	
marked as compliant	
prevented from accessing company resources	
reported with a low device threat	

**Explanation:**

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android>