

# Top Exam MS-102 Papers - How to Prepare for Microsoft MS-102 In Short Time



P.S. Free 2026 Microsoft MS-102 dumps are available on Google Drive shared by PDF4Test: <https://drive.google.com/open?id=1WiUjGhhqHfiEhFsaeuDyLWWCugy398jD>

Everyone wants to have a good job and decent income. But if they don't have excellent abilities and good major knowledge they are hard to find a decent job. Passing the test MS-102 certification can make you realize your dream and find a satisfied job. Our study materials are a good tool that can help you pass the exam easily. You will feel convenient if you buy our product not only because our MS-102 Exam Prep is of high pass rate but also our service is also perfect. What's more, our update can provide the latest and most useful MS-102 exam guide to you, in order to help you learn more and master more.

## Microsoft MS-102 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Manage security and threats by using Microsoft Defender XDR: This topic discusses how to use Microsoft Defender portal to manage security reports and alerts. It also focuses on usage of Microsoft Defender for Office 365 to implement and manage email and collaboration protection. Lastly, it discusses the usage of Microsoft Defender for Endpoint for the implementation and management of endpoint protection.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>Deploy and manage a Microsoft 365 tenant: Management of roles in Microsoft 365 and management of users and groups are discussion points of this topic. It also focuses on implementing and managing a Microsoft 365 tenant.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>Manage compliance by using Microsoft Purview: Implementation of Microsoft Purview information protection and data lifecycle management is discussed in this topic. Moreover, questions about implementing Microsoft Purview data loss prevention (DLP) also appear.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>Implement and manage Microsoft Entra identity and access: In this topic, questions about Microsoft Entra tenant appear. Moreover, it delves into implementation and management of authentication and secure access.</li></ul>

>> Exam MS-102 Papers <<

## Latest MS-102 Training, Reliable MS-102 Practice Questions

With the Microsoft MS-102 practice test, users can reduce stress, and improve their confidence to succeed. The desktop-based Microsoft 365 Administrator (MS-102) practice test software is compatible with Windows only. But the web-based MS-102 Practice Test is compatible with all operating systems.

## Microsoft 365 Administrator Sample Questions (Q524-Q529):

### NEW QUESTION # 524

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.

All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.

You plan to implement self-service password reset (SSPR).

You need to ensure that when a user resets or changes a password, the password syncs with AD DS.

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order.

Each action 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.

Actions	Answer Area
From the Microsoft Entra admin center, configure on-premises integration password writeback.	Step 1: Validate permissions for the Microsoft Entra Connect account.
From the Microsoft Entra admin center, configure the authentication methods for SSPR.	Step 2: <input type="text"/>
From the Microsoft Entra admin center, configure the registration settings for SSPR.	Step 3: <input type="text"/>
Select Group writeback in Microsoft Entra Connect.	
Select Password writeback in Microsoft Entra Connect.	

Answer:

Explanation:

Actions	Answer Area
From the Microsoft Entra admin center, configure on-premises integration password writeback.	Step 1: Validate permissions for the Microsoft Entra Connect account.
From the Microsoft Entra admin center, configure the authentication methods for SSPR.	Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.
From the Microsoft Entra admin center, configure the registration settings for SSPR.	Step 3: Select Password writeback in Microsoft Entra Connect.
Select Group writeback in Microsoft Entra Connect.	
Select Password writeback in Microsoft Entra Connect.	

Explanation:

Actions	Answer Area
From the Microsoft Entra admin center, configure on-premises integration password writeback.	Step 1: Validate permissions for the Microsoft Entra Connect account.
From the Microsoft Entra admin center, configure the authentication methods for SSPR.	Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.
From the Microsoft Entra admin center, configure the registration settings for SSPR.	Step 3: Select Password writeback in Microsoft Entra Connect.
Select Group writeback in Microsoft Entra Connect.	
Select Password writeback in Microsoft Entra Connect.	

### NEW QUESTION # 525

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

- \* Use a file plan to manage retention labels.
- \* Identify, monitor, and automatically protect sensitive information.
- \* Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution 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.

Options	Answer Area
Data loss prevention	Identify, monitor, and automatically protect sensitive information:
Information governance	Capture employee communications for examination by designated reviewers:
Insider risk management	Use a file plan to manage retention labels:
Records management	

**Answer:**

Explanation:

Options	Answer Area
Data loss prevention	Identify, monitor, and automatically protect sensitive information: Data loss prevention
Information governance	Capture employee communications for examination by designated reviewers: Insider risk management
Insider risk management	Use a file plan to manage retention labels: Information governance
Records management	

Explanation:

Identify, monitor, and automatically protect sensitive information:	Data loss prevention
Capture employee communications for examination by designated reviewers:	Insider risk management
Use a file plan to manage retention labels:	Information governance

### NEW QUESTION # 526

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. 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
Anti-malware	Customize the common attachments filter:
Anti-phishing	Enable impersonation protection for sender domains:
Anti-spam	
Safe Attachments	

**Answer:**

Explanation:

Policy Types	Answer Area
<input type="radio"/> Anti-malware	Customize the common attachments filter: <input type="radio"/> Anti-malware
<input type="radio"/> Anti-phishing	Enable impersonation protection for sender domains: <input type="radio"/> Anti-phishing
<input type="radio"/> Anti-spam	
<input type="radio"/> Safe Attachments	

Explanation

A close-up of a question Description automatically generated

Policy Types	Answer Area
<input type="radio"/> Anti-malware	Customize the common attachments filter: <input type="radio"/> Anti-malware
<input type="radio"/> Anti-phishing	Enable impersonation protection for sender domains: <input type="radio"/> Anti-phishing
<input type="radio"/> Anti-spam	
<input type="radio"/> Safe Attachments	

Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

1. Use the Microsoft 365 Defender portal to create anti-malware policies In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies

& Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use <https://security.microsoft.com/antimalwarev2>

2. On the Anti-malware page, select Create to open the new anti-malware policy wizard.

On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

3. When you're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)

5. On the Protection settings page, configure the following settings:

Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains.

Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure>

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

### NEW QUESTION # 527

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

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

Answer: A

### NEW QUESTION # 528

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.

You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for identity Contoso Administrators	None
User2	Defender for identity Contoso Users	None
User3	None	Security administrator
User4	Defender for identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identity sensors.

Solution: You instruct User4 to modify the Defender for identity sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Answer: A



• • • • •

**Latest MS-102 Training:** <https://www.pdf4test.com/MS-102-dump-torrent.html>

- 2026 Latest PDF4Test MS-102 PDF Dumps and MS-102 Exam Engine Free Share: <https://drive.google.com/open?id=1WiUjGhhqHfrEhFsacuDyLWWCugy398jD>

2026 Latest PDF4Test MS-102 PDF Dumps and MS-102 Exam Engine Free Share: <https://drive.google.com/open?id=1WiUjGhhqHfrEhFsacuDyLWWCugy398jD>