

Microsoft - Perfect MS-102 Latest Exam Camp



BONUS!!! Download part of Exams4sures MS-102 dumps for free: https://drive.google.com/open?id=1ie_1-rHc4AnwG8qxjam2OeHt5i_7IF8T

We also offer a free demo version that gives you a golden opportunity to evaluate the reliability of the Microsoft 365 Administrator (MS-102) exam study material before purchasing. Vigorous practice is the only way to ace the Microsoft 365 Administrator (MS-102) test on the first try. And that is what Exams4sures Microsoft MS-102 practice material does. Each format of updated MS-102 preparation material excels in its way and helps you pass the MS-102 examination on the first attempt.

As a high-standard company in the international market, every employee of our MS-102 simulating exam regards protecting the interests of clients as the creed of the job. We know that if we want to make the company operate in the long term, respecting customers is what we must do. Many of our users of the MS-102 Exam Materials are recommended by our previous customers and we will cherish this trust. Our MS-102 practice guide is not only a product you purchase but also a friend who goes with you.

>> MS-102 Latest Exam Camp <<

Fast Download MS-102 Latest Exam Camp & Guaranteed Microsoft MS-102 Exam Success with Excellent MS-102 Testdump

In order to get timely assistance when you encounter problems, our staff will be online 24 hours a day. Regardless of the problem you encountered during the use of MS-102 guide materials, you can send us an email or contact our online customer service. As for the technical issues you are worried about on the MS-102 Exam Questions, we will also provide professional personnel to assist you remotely. And if you have any problem on our MS-102 learning guide, you can contact with us via email or online.

Microsoft MS-102 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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.
Topic 2	<ul style="list-style-type: none">• 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.
Topic 3	<ul style="list-style-type: none">• 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.

Topic 4	<ul style="list-style-type: none"> 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.
---------	---

Microsoft 365 Administrator Sample Questions (Q191-Q196):

NEW QUESTION # 191

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
 Show app and profile configuration progress: Yes
 Allow users to collect logs about installation errors: Yes
 Only show page to devices provisioned by out-of-box experience (OOBE): No
 Assignments: 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.

 Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

NEW QUESTION # 192

You need to meet the technical requirements and planned changes for Intune.

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

NOTE: Each correct selection is worth one point.

Answer Area

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Answer:

Explanation:

Answer Area

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Explanation

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)**
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment**
- Mobile Device Management Authority**

Reference:

<https://docs.microsoft.com/en-us/intune/windows-enroll>

Topic 3, Litware Inc.

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

Devices without an assigned compliance policy show a status of Compliant.

User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.

Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.

Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.

Implement data loss prevention (DLP) policies to protect confidential information.

Grant User2 permissions to review the audit logs of the litware.com tenant.

Deploy new devices to the Seattle office as shown in the following table.

Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

Implement a notification system for when DLP policies are triggered.

Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.

Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.

All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.

Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.

A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.

User2 must be granted the permissions to review audit logs for the following activities:

- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD

Users must be able to apply sensitivity labels to documents by using Office for the web.

Windows Autopilot must be used for device provisioning, whenever possible.

A DLP policy must be created to meet the following requirements:

- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.

The principle of least privilege must be used.

NEW QUESTION # 193

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

- A. Microsoft Entra conditional access
- B. Microsoft Entra password protection
- C. a Microsoft Intune device configuration profile
- D. a Microsoft Intune device compliance policy

Answer: A

NEW QUESTION # 194

You have a Microsoft 365 E5 subscription.

All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.

You need to meet the following requirements:

- * View an assessment of the device configurations against the Center for Internet Security (CIS) v1.0.0 benchmark.
- * Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.

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

Answer Area

The screenshot shows the Microsoft Defender for Endpoint console. It features two dropdown menus. The first dropdown, labeled "To view the device configuration assessment:", has four options: "Create a baseline assessment profile.", "Add a connected application.", "Create a baseline assessment profile." (highlighted in blue), and "Filter the Vulnerable devices report.". The second dropdown, labeled "To protect C:\Folder1, enable:", has four options: "Controlled folder access" (highlighted in blue), "Controlled folder access", "Exploit protection", and "Removable storage protection".

Answer:

Explanation:

Answer Area

This is a detailed view of the configuration options shown in the previous screenshot. The "To view the device configuration assessment:" dropdown is open, showing "Create a baseline assessment profile." selected. The "To protect C:\Folder1, enable:" dropdown is also open, showing "Controlled folder access" selected.

Explanation

Answer Area

This is another view of the configuration options, showing the "To view the device configuration assessment:" dropdown with "Create a baseline assessment profile." selected and the "To protect C:\Folder1, enable:" dropdown with "Controlled folder access" selected.

NEW QUESTION # 195

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.

Answer Area

The screenshot shows a list of compliance solutions on the left and three requirements on the right. The solutions are: "Data loss prevention", "Information governance", "Insider risk management", and "Records management". The requirements are: "Identify, monitor, and automatically protect sensitive information:", "Capture employee communications for examination by designated reviewers:", and "Use a file plan to manage retention labels:". Each requirement has an empty text box next to it for a solution to be dragged.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw,
entrepreneurshiprally.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New MS-102 dumps are available on Google Drive shared by Exams4sures: https://drive.google.com/open?id=1ie_1-rHc4AnwG8qxjam2OeHt5i_7IF8T