

# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam



### NEW QUESTION 1

- (Exam Topic 1)

You need to meet the Intune requirements for the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

|                          |                              |
|--------------------------|------------------------------|
| <input type="checkbox"/> | Device settings              |
| <input type="checkbox"/> | Mobility (MDM and MAM)       |
| <input type="checkbox"/> | Organizational relationships |
| <input type="checkbox"/> | User settings                |

Settings to configure in Intune:

|                          |                                    |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Device compliance                  |
| <input type="checkbox"/> | Device configuration               |
| <input type="checkbox"/> | Device enrollment                  |
| <input type="checkbox"/> | Mobile Device Management Authority |

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

References:

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

### NEW QUESTION 2

- (Exam Topic 1)

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Intune admin center, add User1 as a device enrollment manager.
- D. From the Intune admin center, configure the Enrollment restrictions.

**Answer:** C

#### Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

### NEW QUESTION 3

- (Exam Topic 1)

On which server should you install the Azure ATP sensor?

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

**Answer:** A

#### Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning>

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

### NEW QUESTION 4

- (Exam Topic 1)

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- A. 1
- B. 4
- C. 7
- D. 31

**Answer:** B

#### Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

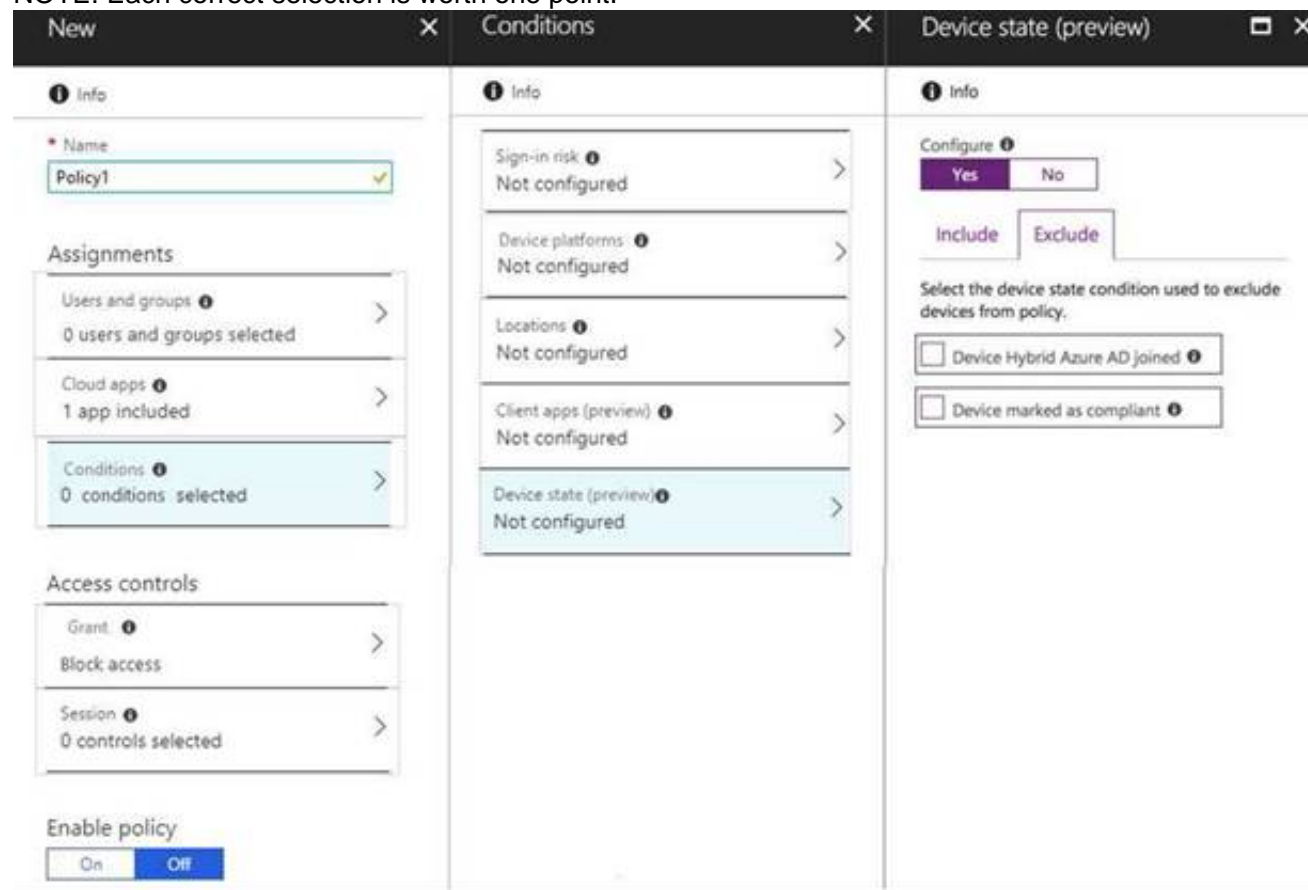
### NEW QUESTION 5

- (Exam Topic 1)

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Suggested Answer

References: <https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

### NEW QUESTION 6

- (Exam Topic 1)

You need to meet the compliance requirements for the Windows 10 devices.

What should you create from the Intune admin center?

- A. a device compliance policy
- B. a device configuration profile
- C. an application policy
- D. an app configuration policy

**Answer: C**

### NEW QUESTION 7

- (Exam Topic 2)

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection
- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

**Answer: B**

#### Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-condition> states clearly that Sign-in risk

### NEW QUESTION 8

- (Exam Topic 2)

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

**NEW QUESTION 9**

- (Exam Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

From the Security & Compliance admin center, perform a search by using:

|                        |
|------------------------|
| ▼                      |
| Audit log              |
| Data governance events |
| DLP policy matches     |
| eDiscovery             |

Filter by:

|            |
|------------|
| ▼          |
| Activity   |
| Detail     |
| Item       |
| User agent |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

**NEW QUESTION 10**

- (Exam Topic 3)

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements. What should you do?

- A. From the Microsoft 365 security center, configure an alert policy.
- B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
- C. From the Microsoft 365 admin center, configure a Briefing email.
- D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-world>

**NEW QUESTION 10**

- (Exam Topic 3)

You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

- A. Replace
- B. Enable redirect
- C. Block
- D. Dynamic Delivery

**Answer:** D

**Explanation:**

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/sa>

**NEW QUESTION 12**

- (Exam Topic 3)

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements. What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure:  ▼

|  |                         |
|--|-------------------------|
| Device configuration profiles                      | Enrollment restrictions |
| The mobile device management (MDM) user scope      |                         |
| The mobile application management (MAM) user scope |                         |

Group:  ▼

|              |
|--------------|
| UserGroup1   |
| UserGroup2   |
| DeviceGroup1 |
| DeviceGroup2 |

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated with medium confidence

Reference:

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

**NEW QUESTION 16**

- (Exam Topic 3)

You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

- A. From Compliance policies, modify the Notifications settings.  
B. From Locations, create a new location for noncompliant devices.  
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.  
D. Modify the Compliance policy settings.

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 21**

- (Exam Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements. To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group:  ▼

|                       |
|-----------------------|
| Reviewer              |
| Global reader         |
| Data Investigator     |
| Compliance Management |

Tool:  ▼

|                               |
|-------------------------------|
| Exchange admin center         |
| SharePoint admin center       |
| Microsoft 365 admin center    |
| Microsoft 365 security center |

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vi>

**NEW QUESTION 23**

- (Exam Topic 3)

You plan to implement the endpoint protection device configuration profiles to support the planned changes. You need to identify which devices will be supported, and how many profiles you should implement.

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

NOTE: Each correct selection is worth one point.



Supported devices:

|   |
|---|
| Device1 only                                    |
| Device1 and Device2 only                        |
| Device1 and Device3 only                        |
| Device1, Device2, and Device3                   |
| Device1, Device4, and Device5                   |
| Device1, Device2, Device3, Device4, and Device5 |

Number of required profiles:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create>

**NEW QUESTION 24**

- (Exam Topic 4)

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication  
 B. pass-through authentication and seamless SSO  
 C. password hash synchronization and seamless SSO  
 D. password hash synchronization

**Answer:** C

**Explanation:**

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365. Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

**NEW QUESTION 28**

- (Exam Topic 5)

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.

| 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"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

| 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"/> |

NEW QUESTION 29

- (Exam Topic 5)  
You have a Microsoft 365 E5 tenant.  
The Microsoft Secure Score for the tenant is shown in the following exhibit.

Microsoft Secure Score

|   |  |              |                  |
|---|--|--------------|------------------|
| Overview  | Improvement actions  | History      | Metrics & trends |
| Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours. |  |              |                  |
| ⌵ Export  | 12 items   | 🔍 Search     | ⌵ Filter         |
| Applied filters:  |  |              |                  |
| Rank ⌵  | Improvement action   | Score impact | Points achieved  |
| 1   | Require MFA for administrative roles                             | +16.95%      | 0/10             |
| 2   | Ensure all users can complete multi-factor authentication for... | +15.25%      | 0/9              |
| 3   | Enable policy to block legacy authentication                     | +13.56%      | 0/8              |
| 4   | Turn on user risk policy   | +11.86%      | 0/7              |
| 5   | Turn on sign-in risk policy                                      | +11.86%      | 0/7              |
| 6   | Do not allow users to grant consent to unmanaged applicatio...   | +6.78%       | 0/4              |
| 7   | Enable self-service password reset                               | +1.69%       | 0/1              |
| 8   | Turn on customer lockbox feature                                 | +1.69%       | 0/1              |
| 9   | Use limited administrative roles                                 | +1.69%       | 0/1              |
| 10  | Designate more than one global admin                             | +1.69%       | 0/1              |

You plan to enable Security defaults for Azure Active Directory (Azure AD). Which three improvement actions will this affect?

- A. Require MFA for administrative roles.
- B. Ensure all users can complete multi-factor authentication for secure access
- C. Enable policy to block legacy authentication
- D. Enable self-service password reset
- E. Use limited administrative roles

Answer: ABC

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

NEW QUESTION 34

- (Exam Topic 5)  
Your network contains an Active Directory forest named contoso.local.  
You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months. You need to prepare for the planned move to Microsoft 365.  
 What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.
- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

**Answer:** D

**Explanation:**

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization>

**NEW QUESTION 39**

- (Exam Topic 5)

You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

A user named User1 stores documents in Microsoft OneDrive.

You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

https://

|                      |                      |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds>

**NEW QUESTION 40**

- (Exam Topic 5)

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

| Name  | Azure Active Directory (Azure AD) role | Microsoft Store for Business role | Member of |
|-------|--|-----------------------------------|-----------|
| User1 | Application administrator              | Basic Purchaser                   | Group1    |
| User2 | None                                   | Purchaser                         | Group2    |
| User3 | None                                   | Basic Purchaser                   | Group3    |

You perform the following actions:

- > Provision the private store in Microsoft Store for Business.
- > Add an app named App1 to the private store.
- > Set Private store availability for App1 to Specific groups, and then select 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.

| Statements                                     | Yes                   | No                    |
|--|-----------------------|-----------------------|
| User1 can install App1 from the private store. | <input type="radio"/> | <input type="radio"/> |
| User2 can install App1 from the private store. | <input type="radio"/> | <input type="radio"/> |
| User3 can install App1 from the private store. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated



Reference:

<https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#priva>

#### NEW QUESTION 42

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

##### Answer Area

Social engineering technique:

▼

Credential harvest  
Link to malware  
Malware attachment

Training experience:

▼

Identity Theft  
Mass Market Phishing  
Web Phishing

- A. Mastered
- B. Not Mastered

**Answer:** A

##### Explanation:

Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available: Credential Harvest

Malware Attachment Link to Malware Etc.

Box 2: Mass Market Phishing Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-start>

#### NEW QUESTION 43

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must

NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

##### Answer Area

▼

Connect-AzureAD  
Connect-MgGraph  
Connect-MSOLService

-Scopes User.ReadWrite.All, Organization.Read.All

\$E3 =

▼

Get-AzureADUser  
Get-MgSubscribedSku  
Get-MSOLAccountSKU

| Where SkuPartNumber -eq 'EnterprisePack'

\$disabledPlans = \$E3.ServicePlans | Where ServicePlanName -in ("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

\$LicenseOptions= @(

@{

SkuId = \$E3.SkuId

DisabledPlans = \$disabledPlans

}

)

▼

Set-AzureADUser  
Set-MgUserLicense  
Set-MSOLUser

-UserId User1@contoso.com -AddLicenses \$LicenseOptions -RemoveLicenses @(

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant. Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

Set-MgUserLicense -UserId \$userUPN -AddLicenses @{Skuld = "<Skuld>"} -RemoveLicenses @() This example assigns a license from the SPE\_E5 (Microsoft 365 E5) licensing plan to the unlicensed user

belindan@litwareinc.com:

\$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE\_E5'

Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{Skuld = \$e5Sku.Skuld}

-RemoveLicenses @()

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365>

**NEW QUESTION 44**

- (Exam Topic 5)

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:** D

**Explanation:**

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.

| Report                  | Public | GCC              | GCC-High         | DoD              | Office 365 operated by 21Vianet |
|-------------------------|--------|------------------|------------------|------------------|---------------------------------|
| Microsoft browser usage | Yes    | N/A <sup>1</sup> | N/A <sup>1</sup> | N/A <sup>1</sup> | N/A <sup>1</sup>                |
| Email activity          | Yes    | Yes              | Yes              | Yes              | Yes                             |
| Email apps usage        | Yes    | Yes              | Yes              | Yes              | Yes                             |
| Mailbox usage           | Yes    | Yes              | Yes              | Yes              | Yes                             |
| Office activations      | Yes    | Yes              | Yes              | Yes              | Yes                             |

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

**NEW QUESTION 49**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Policy type:  These are the selections for Policy type.

Filter type:  These are the selections for Filter type.

Filter type:  These are the selections for Filter type.

Filter type:  These are the selections for Filter type.

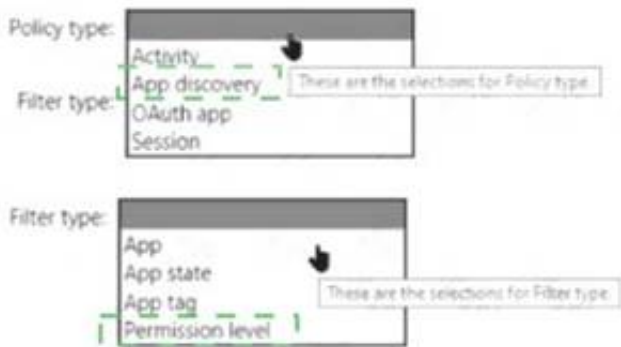
Filter type:  These are the selections for Filter type.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 54

- (Exam Topic 5)

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

| Name    | Operating system                                | Configuration     |
|---------|---|-------------------|
| Server1 | Windows Server 2022                             | Domain controller |
| Server2 | Windows Server 2016                             | Member server     |
| Server3 | Server Core installation of Windows Server 2022 | Member server     |

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install:

Server:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a

light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

\* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install> <https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites>

NEW QUESTION 55

- (Exam Topic 5)

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.



Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com. You plan to install Azure AD Connect on a member server and implement pass-through authentication. You need to prepare the environment for the planned implementation of pass-through authentication. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From a domain controller install an Authentication Agent
- B. From the Microsoft Entra admin center, configure an authentication method.
- C. From Active Director,' Domains and Trusts add a UPN suffix
- D. Modify the email address attribute for each user account.
- E. From the Microsoft Entra admin center, add a custom domain name.
- F. Modify the User logon name for each user account.

**Answer:** ABE

**Explanation:**

Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites

Ensure that the following prerequisites are in place. In the Entra admin center

\* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.

(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.

(A) In your on-premises environment

\* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.

\* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.

\* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.

\* 4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User

sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account.

Not F. Modify the User logon name for each user account. Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

**NEW QUESTION 59**

- (Exam Topic 5)

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.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role. Does this meet the goal?

A. Yes

B. No

**Answer:** B

**Explanation:**

You need to assign the Security Administrator role. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi>

**NEW QUESTION 60**

- (Exam Topic 5)

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

| Name    | Platform   | BitLocker Drive Encryption (BitLocker) | Member of      |
|---------|------------|--|----------------|
| Device1 | Windows 10 | Disabled                               | Group3         |
| Device2 | Windows 10 | Disabled                               | Group2, Group3 |
| Device3 | Windows 10 | Disabled                               | Group2         |

The device compliance policies in Endpoint Manager are configured as shown in the following table.

| Name    | Platform             | Require BitLocker | Assigned |
|---------|----------------------|-------------------|----------|
| Policy1 | Windows 10 and later | Require           | Yes      |
| Policy2 | Windows 10 and later | Not configured    | Yes      |
| Policy3 | Windows 10 and later | Require           | No       |

The device compliance policies have the assignments shown in the following table.

| Name    | Assigned to |
|---------|-------------|
| Policy1 | Group3      |
| Policy2 | 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                    |
|-----------------------|-----------------------|-----------------------|
| Device1 is compliant. | <input type="radio"/> | <input type="radio"/> |
| Device2 is compliant. | <input type="radio"/> | <input type="radio"/> |
| Device3 is compliant. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements            | Yes                              | No                               |
|-----------------------|----------------------------------|----------------------------------|
| Device1 is compliant. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Device2 is compliant. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Device3 is compliant. | <input checked="" type="radio"/> | <input type="radio"/>            |

NEW QUESTION 64

- (Exam Topic 5)

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.

Actions

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-a>

NEW QUESTION 68

- (Exam Topic 5)

DRAG DROP

You have a Microsoft 365 E5 subscription. Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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

- From the Microsoft Endpoint Manager admin center, add a device enrollment manager.
- From the Microsoft Endpoint Manager admin center, download a certificate signing request.
- Upload an Apple MDM push certificate to Microsoft Endpoint Manager.
- Create a certificate from the Apple Push Certificates Portal.
- From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

## Answer Area

- A. Mastered  
B. Not Mastered

**Answer:** A

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>

## NEW QUESTION 71

- (Exam Topic 5)

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

| Name    | Windows 10 edition    | Azure Active Directory (Azure AD) | Mobile device management (MDM) enrollment |
|---------|-----------------------|-----------------------------------|---|
| Device1 | Windows 10 Pro        | Registered                        | Microsoft Intune                          |
| Device2 | Windows 10 Enterprise | Joined                            | Microsoft Intune                          |
| Device3 | Windows 10 Pro        | Joined                            | Not enrolled                              |
| Device4 | Windows 10 Enterprise | Registered                        | Microsoft Intune                          |
| Device5 | Windows 10 Enterprise | Joined                            | Not enrolled                              |

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

- A. Device2 only  
B. Device1 and Device3 only  
C. Device2 and Device4 only  
D. Device2, Device3, and Device5 only  
E. Device1, Device2, Device3, Device4, and Device5

**Answer:** C

## NEW QUESTION 73

- (Exam Topic 5)

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule  
B. an allowed/blocked list rule  
C. an alert suppression rule  
D. an indicator

**Answer:** D

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

## NEW QUESTION 77

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant

You create a data loss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.

To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this beta capability. [Take note about the prerequisites](#)

| Status                       | Location                        | Included                            | Excluded |
|------------------------------|---------------------------------|-------------------------------------|----------|
| <input type="checkbox"/> Off | Exchange email                  | <input checked="" type="checkbox"/> |          |
| <input type="checkbox"/> Off | SharePoint sites                |                                     |          |
| <input type="checkbox"/> Off | OneDrive accounts               | <input checked="" type="checkbox"/> |          |
| <input type="checkbox"/> Off | Teams chat and channel messages |                                     |          |
| <input type="checkbox"/> Off | Devices                         |                                     |          |
| <input type="checkbox"/> Off | Microsoft Cloud App Security    |                                     |          |
| <input type="checkbox"/> Off | On-premises repositories        |                                     |          |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this beta capability. [Take note about the prerequisites](#)

| Status                       | Location                        | Included                            | Excluded |
|------------------------------|---------------------------------|-------------------------------------|----------|
| <input type="checkbox"/> Off | Exchange email                  | <input checked="" type="checkbox"/> |          |
| <input type="checkbox"/> Off | SharePoint sites                |                                     |          |
| <input type="checkbox"/> Off | OneDrive accounts               | <input checked="" type="checkbox"/> |          |
| <input type="checkbox"/> Off | Teams chat and channel messages |                                     |          |
| <input type="checkbox"/> Off | Devices                         |                                     |          |
| <input type="checkbox"/> Off | Microsoft Cloud App Security    |                                     |          |
| <input type="checkbox"/> Off | On-premises repositories        |                                     |          |

NEW QUESTION 80

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

| Name  | Priority | Action   |
|-------|----------|--|
| Rule1 | 0        | Notify users by using email and policy tips.<br>Customize the policy tip as Rule1 tip.<br>Disable user overrides.                                    |
| Rule2 | 1        | Notify users by using email and policy tips.<br>Customize the policy tip as Rule2 tip.<br>Restrict access to the content.<br>Disable user overrides. |
| Rule3 | 2        | Notify users by using email and policy tips.<br>Customize the policy tip as Rule3 tip.<br>Restrict access to the content.<br>Enable user overrides.  |
| Rule4 | 3        | Notify users by using email and policy tips.<br>Customize the policy tip as Rule4 tip.<br>Restrict access to the content.<br>Disable user overrides. |

Site1 contains the files shown in the following table.

| Name       | Matched DLP rule    |
|------------|---------------------|
| File1.docx | Rule1, Rule2, Rule3 |
| File2.docx | Rule1, Rule3, Rule4 |

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx: 

Rule1 tip only

Rule2 tip only

Rule3 tip only

Rule1 tip and Rule2 tip only

Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx: 

Rule1 tip only

Rule3 tip only

Rule4 tip only

Rule1 tip and Rule4 tip only

Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only  
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.  
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.  
Box 2: Rule1 tip only  
Note: User Override support  
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).  
It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.  
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched. Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp> <https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips>

NEW QUESTION 81

- (Exam Topic 5)  
You have a Microsoft 365 tenant that contains the groups shown in the following table.

| Name   | Type                  |
|--------|-----------------------|
| Group1 | Distribution          |
| Group2 | Mail-enabled security |
| Group3 | Security              |

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

- A. Group3 only
- B. Group1 and Group3 only
- C. Group2 and Group3 only
- D. Group1. Group2. and Group3

Answer: A

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile> <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

NEW QUESTION 83

- (Exam Topic 5)  
You have a Microsoft 365 E5 subscription.  
Users have the devices shown in the following table.

| Name    | Platform   | Owner | Enrolled in Microsoft Endpoint Manager |
|---------|------------|-------|--|
| Device1 | Android    | User1 | Yes                                    |
| Device2 | Android    | User1 | No                                     |
| Device3 | iOS        | User1 | No                                     |
| Device4 | Windows 10 | User2 | Yes                                    |
| Device5 | Windows 10 | User2 | No                                     |
| Device6 | iOS        | User2 | Yes                                    |

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

- A. Device1, Device4, and Device6
- B. Device2, Device3, and Device5
- C. Device1, Device2, Device3, and Device6
- D. Device1, Device2, Device4, and Device5

**Answer:** C

**Explanation:**

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

**NEW QUESTION 84**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

**Answer:** B

**Explanation:**

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- > Windows 10
- > macOS

Other incorrect answer options you may see on the exam include the following:

- > Android Enterprise
- > Windows 8.1 Reference:

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

**NEW QUESTION 85**

- (Exam Topic 5)

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

**Answer:** A

**NEW QUESTION 86**

- (Exam Topic 5)

HOTSPOT

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

| Name  | Role         |
|-------|--------------|
| User1 | Global admin |
| User2 | None         |
| User3 | None         |



You provision the private store in Microsoft Store for Business.  
 You assign Microsoft Store for Business roles to the users as shown in the following table.

| Name  | Role            |
|-------|-----------------|
| User1 | None            |
| User2 | Purchaser       |
| User3 | Basic Purchaser |

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.  
 Which users should you identify? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, text, application Description automatically generated  
 Reference:  
<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business> <https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol>

**NEW QUESTION 87**  
 - (Exam Topic 5)

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

| Name    | Platform   |
|---------|------------|
| Device1 | Windows 10 |
| Device2 | Android    |
| Device3 | iOS        |

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, application Description automatically generated  
 Reference:  
<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure> <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

**NEW QUESTION 91**  
 - (Exam Topic 5)



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

| Name   | Member of Microsoft 365 role group                              |
|--------|---|
| Admin1 | Content Explorer List viewer<br>Content Explorer Content viewer |
| Admin2 | Security Administrator<br>Content Explorer List Viewer          |

You have labels in Microsoft 365 as shown in the following table.

| Name   | Type        |
|--------|-------------|
| Label1 | Sensitivity |
| Label2 | Retention   |

The content in Microsoft 365 is assigned labels as shown in the following table.

| Name  | Type                             | Label  |
|-------|----------------------------------|--------|
| File1 | File in SharePoint Online        | Label1 |
| Mail1 | Email message in Exchange Online | Label2 |

You have labels In Microsoft 365 as shown in the following table.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

| Statements  | Yes                   | No                    |
|---|-----------------------|-----------------------|
| Admin1 can view the contents of File1 by using Content explorer.            | <input type="radio"/> | <input type="radio"/> |
| Admin2 can view the contents of File1 by using Content explorer.            | <input type="radio"/> | <input type="radio"/> |
| Admin2 can use Content explorer to verify that Label2 is assigned to Mail1. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| Admin1 can view the contents of File1 by using Content explorer.            | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can view the contents of File1 by using Content explorer.            | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin2 can use Content explorer to verify that Label2 is assigned to Mail1. | <input type="radio"/>            | <input checked="" type="radio"/> |

NEW QUESTION 96

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

- > Assignments: All users
- > Controls: Require Azure AD multifactor authentication registration
- > Enforce Policy: On
- > On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

| User  | Date     |
|-------|----------|
| User1 | August 5 |
| User2 | August 7 |

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

User1: 

▼

August 6

August 17

August 19

September 3

September 5

User2: 

▼

August 8

August 17

August 19

August 21

September 7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi-Factor Authentication, then the user must be able to pass that MFA request.

Box 2: August 21 Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

NEW QUESTION 99

- (Exam Topic 5)

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

| Name                     | Score | Status     | Assessment progress | Your improvement actions | Microsoft actions    | Group  | Product       | Regulation               |
|--------------------------|-------|------------|---------------------|--------------------------|----------------------|--------|---------------|--------------------------|
| SP800                    | 15444 | Incomplete | 72%                 | 3 of 450 completed       | 887 of 887 completed | Group1 | Microsoft 365 | NIST 800-53              |
| Data Protection Baseline | 14370 | Incomplete | 70%                 | 3 of 489 completed       | 835 of 835 completed | Group2 | Microsoft 365 | Data Protection Baseline |

The SP800 assessment has the improvement actions shown in the following table.

| Improvement action  | Test status | Impact    | Points achieved | Regulations                           |
|---|-------------|-----------|-----------------|---------------------------------------|
| Establish a threat intelligence program                   | None        | +9 points | 0/9             | NIST 800-53, Data Protection Baseline |
| Establish and document a configuration management program | None        | +9 points | 0/9             | NIST 800-53, Data Protection Baseline |

You perform the following actions:

> For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

> Enable multi-factor authentication (MFA) for all users.

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                    |
|---|-----------------------|-----------------------|
| Establish a threat intelligence program will appear as Implemented in the SP800 assessment. | <input type="radio"/> | <input type="radio"/> |
| The SP800 assessment score will increase by 54 points.                                      | <input type="radio"/> | <input type="radio"/> |
| The Data Protection Baseline score will increase by 9 points.                               | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, text Description automatically generated

Reference:

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

**NEW QUESTION 100**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.

You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

- A. scope tags
- B. device configuration profiles
- C. device categories
- D. device compliance policies

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

**NEW QUESTION 104**

- (Exam Topic 5)

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: D**

**NEW QUESTION 106**

- (Exam Topic 5)

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.

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628be>

**NEW QUESTION 109**

- (Exam Topic 5)

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.

| 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"/> |

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 112**

- (Exam Topic 5)

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

| Name  | Member of | Azure Active Directory (Azure AD) role |
|-------|-----------|--|
| User1 | Group1    | Global administrator                   |
| User2 | Group2    | Cloud device administrator             |

You configure an Enrollment Status Page profile as shown in the following exhibit.

## Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

|  |   |
|--|---|
| Show app and profile installation progress.  | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Show time limit error when installation takes longer than specified number of minutes. | <input type="text" value="60"/>                               |
| Show custom message when time limit error occurs.                                      | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow users to collect logs about installation errors.                                 | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Only show page to devices provisioned by out-of-box experience (OOBE)                  | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Block device use until all apps and profiles are installed                             | <input type="radio"/> Yes <input checked="" type="radio"/> No |

You assign the policy to Group1.

You purchase the devices shown in the following table.

| Name    | Platform   |
|---------|------------|
| Device1 | Windows 10 |
| Device2 | Android    |

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 performs the initial device enrollment for Device1, the Enrollment Status Page will show. | <input type="radio"/> | <input type="radio"/> |
| If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show. | <input type="radio"/> | <input type="radio"/> |
| If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 115**

- (Exam Topic 5)

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

- A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
- B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
- C. From the Microsoft 365 admin center, modify Organization information.
- D. From the Microsoft 365 admin center, modify Help desk information.

**Answer:** A

**Explanation:**

Reference:

<https://systemcenterdudes.com/intune-company-portal-customization/>

**NEW QUESTION 119**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online. You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

- A. set-unifiedGroup
- B. Set-Labelpolicy
- C. Execute-AzureAdLabelSync
- D. Add-UnifiedGroupLinks

**Answer:** C

**NEW QUESTION 123**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a trainable classifier
- B. a sensitive info type
- C. an insider risk policy
- D. an adaptive policy scope
- E. a data loss prevention (DLP) policy

**Answer:** AE

**Explanation:**

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers



Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels  
Auto-apply retention label policy based on a condition Communication compliance  
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically. Data loss prevention  
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).  
Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

**NEW QUESTION 127**

- (Exam Topic 5)  
Your company has multiple offices.  
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.  
You need to ensure that the local administrators can manage only the devices in their respective office. What should you use?

- A. scope tags
- B. configuration profiles
- C. device categories
- D. conditional access policies

**Answer:** A

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

**NEW QUESTION 129**

- (Exam Topic 5)  
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to automatically label the documents on Site1 that contain credit card numbers.  
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**

Create a sensitivity label.

Create an auto-labeling policy.

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Publish the label.

Create a retention label.

Wait eight hours, and then turn on the policy.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application, email Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-labe> <https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w>

**NEW QUESTION 132**

- (Exam Topic 5)  
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

**Answer:** C

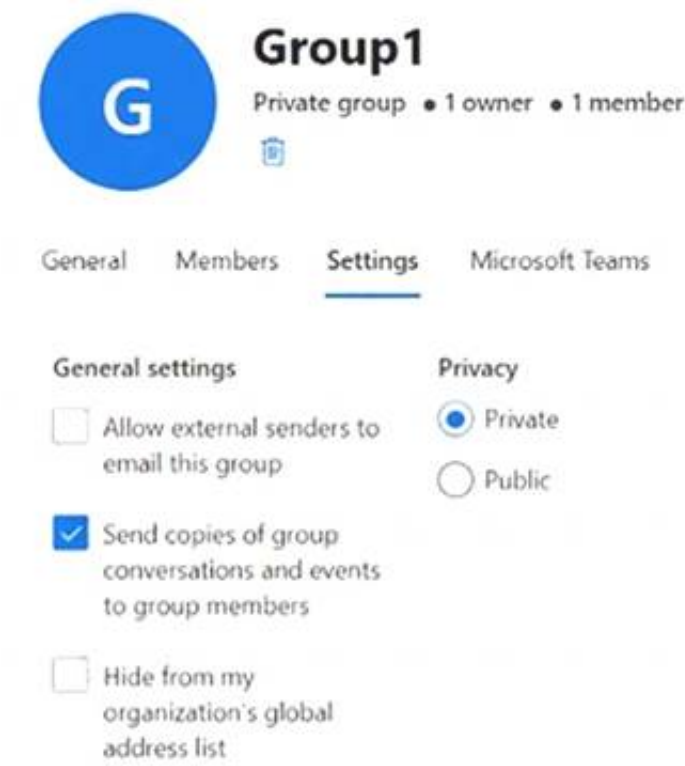
**Explanation:**

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-m>

**NEW QUESTION 135**

- (Exam Topic 5)  
 HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1. What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Action:

Add User1 to the subscription as an active user.

For Group1, change the Privacy setting to Public.

For Group1, select Allow external senders to email this group.

Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center

The Exchange admin center

The Microsoft 365 admin center

The Microsoft Purview compliance portal

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Invite User1 to collaborate with your organization as a guest.  
 To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps. Navigate with your Web browser to <https://admin.microsoft.com>.  
 On the left pane, click on "Users", then click "Guest Users".  
 On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.  
 On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.  
 Box 2: The Microsoft Entra admin center  
 Microsoft Entra admin center unites Azure AD with family of identity and access products  
 Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions

Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

Reference:

<https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users> <https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-ac>

### NEW QUESTION 136

- (Exam Topic 5)

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

Perform a configuration assessment of the operating system

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Detect operating system vulnerabilities

Perform a configuration assessment of the operating system

### NEW QUESTION 138

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription 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 publish a sensitivity label named Label1. To which groups can you publish Label1?

- A. Group1 only  
 B. Group1 and Group2 only  
 C. Group1 and Group4 only  
 D. Group1, Group2, and Group3 only  
 E. Group1 Group2, Group3, and Group4

**Answer:** A

**Explanation:**

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>

#### NEW QUESTION 141

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.

You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

|                                |  |
|--------------------------------|--|
| To configure Azure AD Connect: | <input type="checkbox"/> Configure hybrid Azure AD join.<br><input type="checkbox"/> Enable device writeback.<br><input type="checkbox"/> Enable password hash synchronization.              |
| To configure the domain:       | <input type="checkbox"/> Add an alternative UPN suffix.<br><input type="checkbox"/> Register a service connection point.<br><input type="checkbox"/> Register a service principal name (SPN) |

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

|                                |  |
|--------------------------------|--|
| To configure Azure AD Connect: | <input checked="" type="checkbox"/> Configure hybrid Azure AD join.<br><input checked="" type="checkbox"/> Enable device writeback.<br><input checked="" type="checkbox"/> Enable password hash synchronization. |
| To configure the domain:       | <input checked="" type="checkbox"/> Add an alternative UPN suffix.<br><input type="checkbox"/> Register a service connection point.<br><input type="checkbox"/> Register a service principal name (SPN)          |

#### NEW QUESTION 144

- (Exam Topic 5)

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.

**Answer: BD**

**Explanation:**

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>

#### NEW QUESTION 147

- (Exam Topic 5)

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:**

Reference:

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



#### NEW QUESTION 151

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center you create a threat management policy. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### NEW QUESTION 153

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices. You enable device clean-up rules.

What can you configure as the minimum number of days before a device is removed automatically?

- A. 10
- B. 30
- C. 45
- D. 90

**Answer: D**

#### NEW QUESTION 154

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

- A. Microsoft Store for Business
- B. Apple Business Manager
- C. Apple iTunes Store
- D. Apple Configurator

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

#### NEW QUESTION 158

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations. Which conditions can you use in the DLP rules of the policy?

- A. sensitive info types
- B. content search queries
- C. keywords
- D. sensitivity labels

**Answer: C**

#### Explanation:

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.

Specific keywords that match a query you create. Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations: Exchange mailboxes

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels)

Teams chats

Teams private channel messages Yammer community messages Yammer user messages Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions>

#### NEW QUESTION 159

- (Exam Topic 5)

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.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role. Does this meet the goal?



- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to assign the Security Administrator role. Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>

**NEW QUESTION 162**

- (Exam Topic 5)

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 copy the Group Policy Administrative Templates from a Windows 10 computer to Server1. Does this meet the goal?

- A. yes
- B. No

**Answer:** A

**NEW QUESTION 163**

- (Exam Topic 5)

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.

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed. Solution: From Device Manager, you view the computer properties. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:  
<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628be>

**NEW QUESTION 167**

- (Exam Topic 5)

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 169**

- (Exam Topic 5)

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   | Yes                   | No                    |
|--|-----------------------|-----------------------|
| On July 15, 2023, Admin1 can reset the password of a user.     | <input type="radio"/> | <input type="radio"/> |
| On June 20, 2023, Admin2 can manage Microsoft Exchange Online. | <input type="radio"/> | <input type="radio"/> |
| On May 1, 2023, Admin3 can reset the password of a user.       | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member. The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible

June 20, 2023 is with the assignment period. The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

Admin3 is member of Group1 and Group2.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

May 1, 2023 is with the assignment period. Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference> <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member>

**NEW QUESTION 170**

- (Exam Topic 5)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

- A. Delete the workspace.
- B. Create a workspace.
- C. Onboard a new device.
- D. Offboard the test devices.

**Answer:** B

**Explanation:**

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

\* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace>

**NEW QUESTION 171**

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1, Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).

You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

- A. Windows 11 and Windows 10 only
- B. Windows 11, Windows 10-Windows8.1.andmacOS
- C. Windows 11 and macOS only
- D. Windows 11 only

E. Windows 11. Windows 10, and Windows8.1 only

**Answer:** C

**NEW QUESTION 172**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### MS-102 Practice Exam Features:

- \* MS-102 Questions and Answers Updated Frequently
- \* MS-102 Practice Questions Verified by Expert Senior Certified Staff
- \* MS-102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* MS-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The MS-102 Practice Test Here](#)**