

## Exam Questions MS-102

Microsoft 365 Administrator Exam

<https://www.2passeasy.com/dumps/MS-102/>



### NEW QUESTION 1

HOTSPOT - (Topic 6)

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

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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

#### Statements

Yes No

Device1 is marked as compliant.

☐ ☐

Device2 is marked as compliant.

☐ ☐

Device3 is marked as compliant.

☐ ☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Statements

Yes No

Device1 is marked as compliant.

☒ ☐

Device2 is marked as compliant.

☒ ☐

Device3 is marked as compliant.

☐ ☒

### NEW QUESTION 2

- (Topic 6)

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

- Assign licenses to users.
- Procure apps from Microsoft Store.
- Manage private store availability for all items.

The solution must use the principle of least privilege.

Which Microsoft Store for Business role should you assign to User1?

- A. Basic Purchaser
- B. Device Guard signer
- C. Admin
- D. Purchaser

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview>

### NEW QUESTION 3

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You need to review metrics for the following: The daily active users in Microsoft Teams Recent Microsoft service issues

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

#### Answer Area

Teams daily active users:

<input type="checkbox"/>	Microsoft Secure Score
<input type="checkbox"/>	Adoption Score
<input type="checkbox"/>	Service health
<input type="checkbox"/>	Usage reports

Recent Microsoft service issues:

<input type="checkbox"/>	Microsoft Secure Score
<input type="checkbox"/>	Adoption Score
<input type="checkbox"/>	Service health
<input type="checkbox"/>	Usage reports

A. Mastered

B. Not Mastered

Answer: A

#### Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity

The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

### NEW QUESTION 4

HOTSPOT - (Topic 6)

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 new capability. [Learn more about the prerequisites](#)

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

- 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 new capability. [Learn more about the prerequisites](#)

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

## NEW QUESTION 5

DRAG DROP - (Topic 6)

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:

#### 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

- Create a sensitivity label.
- 
- Publish the label.
- 
- Create an auto-labeling policy.
- 

### NEW QUESTION 6

HOTSPOT - (Topic 6)

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:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

- 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.

**NEW QUESTION 7**

- (Topic 6)

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

User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.

You need to remove User1 from the Restricted entities list. What should you use?

- A. the Exchange admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft 365 admin center
- D. the Microsoft 365 Defender portal
- E. the Microsoft Entra admin center

**Answer:** D

**Explanation:**

Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam>

**NEW QUESTION 8**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

? Identify when a user's credentials are compromised and shared on the dark web.

? Provide users that have compromised credentials with the ability to self-remediate.

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 identify when users have compromised credentials, configure:

<input type="checkbox"/> A registration policy
<input type="checkbox"/> A sign-in risk policy
<input type="checkbox"/> A user risk policy
<input type="checkbox"/> A multifactor authentication registration policy

To enable self-remediation, select:

<input type="checkbox"/> Generate a temporary password
<input type="checkbox"/> Require multi-factor authentication
<input type="checkbox"/> Require password change

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

#### NEW QUESTION 9

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

**Answer:** D

#### NEW QUESTION 10

- (Topic 6)

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-worldwide>

#### NEW QUESTION 10

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.

You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

- Minimizes user interaction
- Minimizes administrative effort
- Automatically installs corporate apps What should you recommend?

- A. Automated Device Enrollment (ADE)
- B. bring your own device (BYOD) user and device enrollment
- C. Apple Configurator enrollment

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 15

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

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

**Answer:** D

#### Explanation:

Reference:

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

#### NEW QUESTION 17

- (Topic 6)

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 that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

#### NEW QUESTION 18

- (Topic 6)

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- Signs in to Microsoft Exchange Online from an anonymous IP address
- Signs in to Microsoft SharePoint Online from a device in New York City.
- Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

- A. anonymous IP address only
- B. anonymous IP address and atypical travel
- C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
- D. unfamiliar sign-in properties and atypical travel only
- E. anonymous IP address and unfamiliar sign-in properties only

**Answer:** C

#### NEW QUESTION 19

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- Retention period 7 years
- Start the retention period based on: When items were created

You need to prevent the removal of the label once the label is applied to an item. What should you select in the retention label settings?

- A. Retain items even if users delete
- B. Mark items as a record
- C. Mark items as a regulatory record
- D. Retain items forever

**Answer:** B

#### NEW QUESTION 23

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

## Review your settings

**Name** [Edit](#)  
Retention1

**Description for admins** [Edit](#)

**Description for users** [Edit](#)

**File plan descriptors** [Edit](#)  
Reference Id:1  
Business function/department Legal  
Category: Compliance  
Authority type: Legal

**Retention** [Edit](#)  
7 years  
Retain only  
Based on when it was created

[Back](#)[Create this label](#)[Cancel](#)

When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

- A. Create a new label policy
- B. Modify the Authority type setting for Retention!
- C. Modify the Business function/department setting for Retention 1.
- D. Use a file plan CSV template to import Retention1.

**Answer:** A

**Explanation:**

Reference:

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

### NEW QUESTION 28

- (Topic 6)

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You purchase a Microsoft 365 subscription.

You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).

You need to ensure that users can use Seamless SSO from the Windows 10 computers. What should you do?

- A. Join the computers to Azure AD.
- B. Create a conditional access policy in Azure AD.
- C. Modify the Intranet zone settings by using Group Policy.
- D. Deploy an Azure AD Connect staging server.

**Answer:** A

### NEW QUESTION 29

- (Topic 6)

You have a Microsoft 365 subscription.

You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.

What should you do?

- A. Enable Endpoint analytics.
- B. Run the Microsoft 365 network connectivity test on each device.
- C. Enable privileged access.
- D. Configure Support integration.

**Answer:** A

### NEW QUESTION 30

- (Topic 6)

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

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

- A. Group1 only
- B. Group2 only
- C. Site1 only
- D. Group1 and Group2 only
- E. Group1, Group2, and Site1

**Answer:** E

**Explanation:**

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.

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.

When you configure a label policy, you can:

Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

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

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

**NEW QUESTION 33**

- (Topic 6)

You have a Microsoft E5 subscription.

You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.

What should you implement?

- A. Azure AD Privileged Identity Management (PIM)
- B. a conditional access policy
- C. a communication compliance policy
- D. Azure AD Identity Protection
- E. groups that have dynamic membership

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

**NEW QUESTION 38**

HOTSPOT - (Topic 6)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.

Configure

Microsoft Intune

Save

Discard

Delete

MDM user scope ⓘ

None

Some

All

Groups

Select groups

Group1

MDM terms of use URL ⓘ

https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL ⓘ

https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL ⓘ

https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM User scope ⓘ

None

Some

All

Groups

Select groups

Group2

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ

https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL ⓘ

Restore default MAM URLs

You purchase a Windows 10 device named Device1.  
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 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

### NEW QUESTION 43

- (Topic 6)

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 that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:  
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

NEW QUESTION 47

- (Topic 6)  
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 subscription.  
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.  
Solution: From the Endpoint Management admin center, you create a device configuration profile.  
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to create a trusted location and a conditional access policy.

NEW QUESTION 52

HOTSPOT - (Topic 6)  
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these

Sensitive info type	Match accuracy
	minmax
Credit Card Number	85100

Retention labels

1 year

Add

+ Add group

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

DLP1 cannot be applied to [answer choice].

Exchange email

SharePoint sites

OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

both a credit card number and the 1 year label applied

either a credit card number or the 1 year label applied

between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

NEW QUESTION 57

HOTSPOT - (Topic 6)  
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	None
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following exhibit.

Guest user access

Guest user access restrictions ⓘ  
[Learn more](#)

☐ Guest users have the same access as members (most inclusive)

☒ Guest users have limited access to properties and memberships of directory objects

☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ  
[Learn more](#)

☐ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

☒ Only users assigned to specific admin roles can invite guest users

☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ  
[Learn more](#)

☐ Yes ☒ No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ  
[Learn more](#)

Collaboration restrictions

☒ Allow invitations to be sent to any domain (most inclusive)

☐ Deny invitations to the specified domains

☐ Allow invitations only to the specified domains (most restrictive)

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

**NOTE:** Each correct selection is worth one point.

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

**NOTE:** Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User2 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User3 can invite guest users.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can invite guest users.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can invite guest users.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can invite guest users.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 60

- (Topic 6)

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 64

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1. What should you do next?

- A. Connect Defender for Endpoint to Microsoft Intune.
- B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
- C. Create an assessment job.
- D. Download and run an onboarding package.

Answer: C

NEW QUESTION 68

DRAG DROP - (Topic 6)

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

>

<

^

v

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## 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

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

## NEW QUESTION 69

- (Topic 6)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

- A. OneDrive accounts
- B. Exchange email
- C. Teams chat and channel messages
- D. SharePoint sites

Answer: B

## NEW QUESTION 74

HOTSPOT - (Topic 6)

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

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

## Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. [Learn more](#)

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more](#).

**Enable and Target**    Configure

Enable ☒

Include    Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 78

- (Topic 6)  
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe. What should you use?

- A. an indicator
- B. a suppression rule
- C. a device configuration profile

Answer: A

NEW QUESTION 83

HOTSPOT - (Topic 6)  
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:

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

### NEW QUESTION 88

- (Topic 6)

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

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

- A. User1 only
- B. User2 only
- C. User1 and User2 only
- D. User1 and User3 only
- E. User1, User2, and User3

Answer: E

### NEW QUESTION 91

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

NEW QUESTION 92

HOTSPOT - (Topic 6)

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

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

AU1

Members    Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned admins manage group settings.

Add usersAdd groupsUpload users...

Filter

Search this list

<input type="checkbox"/>	Members	Email address	Last sign-in	Member type
<input type="checkbox"/>	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
<input type="checkbox"/>	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General    Assigned    Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

[Learn more about assigning admin roles](#)

Add usersAdd groups

<input type="checkbox"/>	Admin name	Last sign-in	Scope ⓘ
<input type="checkbox"/>	Group1	Unavailable for groups	Organization
<input type="checkbox"/>	Group2	Unavailable for groups	AU1

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 reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 93

- (Topic 6)

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 Active Directory domain. You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 95

- (Topic 6)

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 100

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint

You need to use Defender for Endpoint to block access to a malicious website at [www.contoso.com](http://www.contoso.com).

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

- A. Create a web content filtering policy.
- B. Configure an enforcement scope.
- C. Enable Custom network indicators.
- D. Create an indicator.
- E. Enable automated investigation.

**Answer:** AC

#### NEW QUESTION 101

- (Topic 6)

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 raise the forest functional level to Windows Server 2016.

You copy the Group

Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. yes
- B. No

**Answer:** B

#### NEW QUESTION 102

- (Topic 6)

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

You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.

What should you use?

- A. Microsoft Secure Score
- B. Cloud discovery
- C. Exposure distribution
- D. Threat tracker
- E. Exposure score

Answer: A

#### NEW QUESTION 105

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)

Microsoft Azure Active Directory Connect

Welcome

- Express Settings
- Required Components
- User Sign-in
- Connect to Azure AD
- Sync
  - Connect Directories
  - Azure AD sign-in
  - Domain/OU Filtering**
  - Identifying users
  - Filtering
  - Optional Features
  - Configure

### Domain and OU filtering

Directory: fabrikam.com Refresh Ou/Domain ?

☐ Sync all domains and OUs  
☒ Sync selected domains and OUs

☒ fabrikam.com
 

- ☐ Builtin
- ☐ Computers
- ☐ Domain Controllers
- ☐ ForeignSecurityPrincipals
- ☐ Infrastructure
- ☐ LostAndFound
- ☐ Managed Service Accounts
- ☐ OU1
- ☒ OU2
- ☐ Program Data
- ☐ System
- ☐ Users

Previous Next

You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)

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

### Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

Answer: A

### Explanation:

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized. User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

### NEW QUESTION 109

- (Topic 6)

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 Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory. Does this meet the goal?

- A. Yes  
 B. No

Answer: A

### NEW QUESTION 113

- (Topic 6)

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 Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint 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-worldwide>

## NEW QUESTION 116

HOTSPOT - (Topic 6)

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

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

- Users or workload identities: o Include: Group1

- o Exclude: Group2

- Cloud apps or actions: Include all cloud apps

- Conditions:

- o Include: Any location o Exclude: Montreal

- Access control: Grant access, Require multi-factor authentication User1 is on the multi-factor authentication (MFA) blocked users list.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 121

- (Topic 6)

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort. What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

**Answer:** B

#### Explanation:

Reference:

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

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

#### NEW QUESTION 124

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1

Assignments:

- Users and groups: Group1
- Cloud apps or actions: All cloud apps

? Access controls:

? Grant, require multi-factor authentication

? Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to <b>On</b> .	<input type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to <b>Off</b> .	<input type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to <b>All users</b> .	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

? Conditional Access policies can be enabled in report-only mode.

? During sign-in, policies in report-only mode are evaluated but not enforced.

? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

#### NEW QUESTION 128

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

? MDM user scope: Some

? uk.co.certification.simulator.questionpool.PList@184e72e0

? MAM user scope: Some

? uk.co.certification.simulator.questionpool.PList@184e7360 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
User1 can enroll Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input checked="" type="radio"/>

### NEW QUESTION 131

HOTSPOT - (Topic 6)

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

NOTE: Each correct selection is worth one point.

In Azure:

<input type="checkbox"/> Add and configure the Diagnostics settings for the Azure Activity Log. <input type="checkbox"/> Add and configure an Azure Log Analytics workspace. <input type="checkbox"/> Add an Azure Storage account and Azure Cognitive Search <input type="checkbox"/> Add an Azure Storage account and a file share.
--

On the computers:

<input type="checkbox"/> Create an event subscription. <input type="checkbox"/> Modify the membership of the Event Log Readers group. <input type="checkbox"/> Enroll in Microsoft Endpoint Manager. <input type="checkbox"/> Install the Microsoft Monitoring Agent.
--

A. Mastered

B. Not Mastered

Answer: A

Explanation:

In Azure:

Add and configure the Diagnostics settings for the Azure Activity Log.

Add and configure an Azure Log Analytics workspace.

Add an Azure Storage account and Azure Cognitive Search

Add an Azure Storage account and a file share.

On the computers:

Create an event subscription.

Modify the membership of the Event Log Readers group.

Enroll in Microsoft Endpoint Manager.

Install the Microsoft Monitoring Agent.

NEW QUESTION 134

- (Topic 6)  
You have a Microsoft 365 tenant and a LinkedIn company page.  
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.  
Where can you store data from the LinkedIn connector?

- A. a Microsoft OneDrive for Business folder
- B. a Microsoft SharePoint Online document library
- C. a Microsoft 365 mailbox
- D. Azure Files

Answer: C

Explanation:

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

NEW QUESTION 135

- (Topic 6)  
You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.

Updates

Consent controls updates during updates.

ON

NAME	TYPE	VERSION	AUTOMATIC RESTART	DETAILED UPDATE	STATUS
LOPE-DC	Server	2.117.0.234	<div></div> ON	<div></div> ON	Up to date

Save

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

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

Answer: B

NEW QUESTION 137

HOTSPOT - (Topic 6)  
HOTSPOT

			progress	actions	summary			
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.

Answer Area

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:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 140

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com.

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.

You plan to sync contoso.com to an Azure AD tenant.

You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.

What should you include in the recommendation?

- A. pass-through authentication  
B. conditional access policies  
C. password synchronization  
D. Azure AD Identity Protection policies

Answer: A

Explanation:

Reference:

https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION 145

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)

The device type restriction are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restriction are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer Area

Device limit:

5  
10  
15

Allowed platform:

Android only  
iOS only  
All platforms

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority

#### NEW QUESTION 150

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

? Opening files in Microsoft SharePoint that contain malicious content

? Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Opening files in SharePoint that contain malicious content:

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

A. Mastered

B. Not Mastered

Answer: A

Explanation:

#### Answer Area

Opening files in SharePoint that contain malicious content:

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

#### NEW QUESTION 155

- (Topic 6)

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 Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: A

#### NEW QUESTION 158

- (Topic 6)

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only

B. Microsoft Teams only

C. Microsoft Exchange Online and SharePoint Online only

D. Microsoft Teams and SharePoint Online only

E. Microsoft Teams, Exchange Online, and SharePoint Online

**Answer:** A

**Explanation:**

Privileged access management

Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management>

**NEW QUESTION 162**

- (Topic 6)

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 164**

HOTSPOT - (Topic 6)

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

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You are implementing Microsoft Defender for Endpoint

You need to enable role-based access control (RBAC) to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and which users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

**Answer Area**

Users that can enable RBAC:

Users that will no longer have access to the Microsoft 365 Defender portal:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Users that can enable RBAC:

Admin1 and Admin2 only  
Admin1 only  
Admin1 and Admin2 only  
Admin1, Admin2, and Admin5 only  
Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

Admin3, Admin4, and Admin5 only  
Admin5 only  
Admin3 and Admin4 only  
Admin4 and Admin5 only  
Admin3, Admin4, and Admin5 only

NEW QUESTION 167

- (Topic 6)

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 Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

Answer: A

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 171

HOTSPOT - (Topic 6)

You have a Microsoft 365 Enterprise E5 subscription.

You add a cloud-based app named App1 to the Azure AD enterprise applications list.

You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

App1 policy ✓

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected ✓

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected ✓

Session ⓘ

0 controls selected

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☒ All users

☐ Select users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Enable policy

Report-only On Off ✓

A. Mastered

B. Not Mastered

Answer: A

Explanation:  
Answer Area

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.  
[Learn more](#)

Name \*

App1 policy

What does this policy apply to?

Users and groups

Assignments

Users or workload identities

All users

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Enable policy

Report-only On Off

NEW QUESTION 176

HOTSPOT - (Topic 6)

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)

SharePoint

S Site1

Search Documents

New Upload Quick edit Sync All Documents

Documents

Name	Modified	Modified By
File1.docx	About a minute ago	Prvi
File2.docx	A few seconds ago	Prvi
File3.docx	A few seconds ago	Prvi

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

#### NEW QUESTION 178

- (Topic 6)

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

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations. Which users can the policy protect?

- A. User2 and User4 only  
 B. User1 and User3 only  
 C. User1 only  
 D. User1, User2, User3, and User4

Answer: C

#### NEW QUESTION 182

- (Topic 6)

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.

Policy1

Edit policy

Delete policy

Status

On

Description

Add a description

Severity

Medium

Edit

Category

Information governance

Conditions

Activity is FileModified

Aggregation

Aggregated

Threshold

5 activities

Edit

Window

60 minutes

Scope

All users

Email recipients

User1@M365x082103.onmicrosoft.com

Daily notification limit

25

Edit

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours. How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25

**Answer:** D

#### NEW QUESTION 186

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

- A. an exclusion group
- B. the MFA registration policy
- C. named locations
- D. self-service password reset (SSPR)

**Answer:** D

#### Explanation:

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

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

#### NEW QUESTION 190

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy. What should you do first?

- A. Review the sensitive information in Activity explorer
- B. Turn on the policy
- C. Run the policy in simulation mode
- D. Configure Azure Information Protection analytics

Answer: C

Explanation:

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

NEW QUESTION 191

- (Topic 6)  
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge. What should you create in Microsoft Endpoint Manager?

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

Answer: C

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune>

NEW QUESTION 196

DRAG DROP - (Topic 6)  
Your company purchases a cloud app named App1. You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Cloud App Security admin center, add an app connector.

Sign in to App1.

Create a conditional access policy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

⬅

➡

⬆

⬇

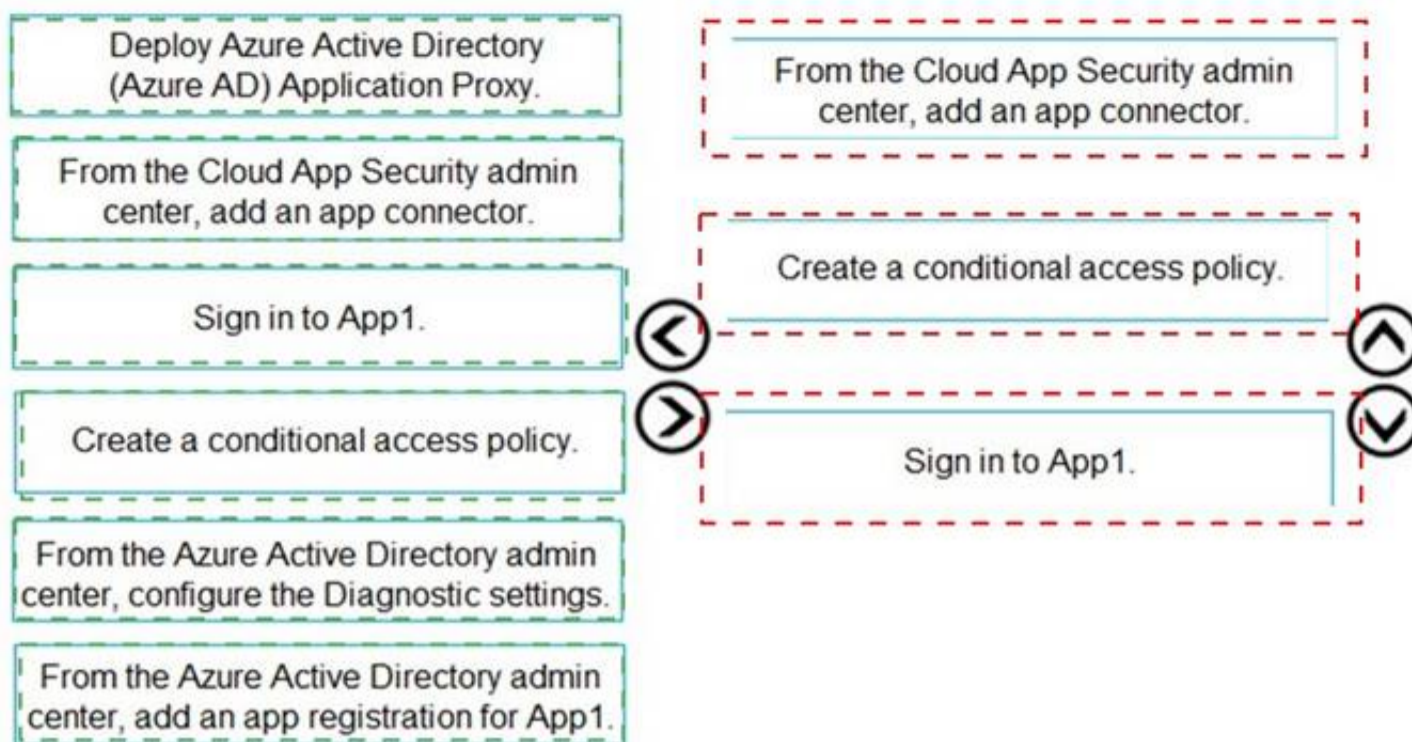
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Actions

## Answer Area



### NEW QUESTION 198

HOTSPOT - (Topic 6)

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00. you create an incident notification rule that has the following configurations:

- Name: Notification!
- Notification settings
  - o Notify on alert severity: Low
  - o Device group scope: All (3)
  - o Details: First notification per incident
- Recipients: User1@contoso.com, User2@contoso.com

At 08:02. you create an incident notification rule that has the following configurations:

- Name: Notification
- Notification settings
  - o Notify on alert severity: Low, Medium
  - o Device group scope: DeviceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

In Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.

NOTE: Each correct selection is worth one point.

### Answer Area

#### Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☐

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☐
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

##### Answer Area

##### Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☒

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☒
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☒

#### NEW QUESTION 199

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.

What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

**Answer:** A

#### NEW QUESTION 202

- (Topic 6)

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 Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.

It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

#### NEW QUESTION 204

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group. Which type of group can you use?

- A. Microsoft 365 only
- B. security only
- C. mail-enabled security and security only
- D. mail-enabled security, Microsoft 365, and security only
- E. distribution, mail-enabled security, Microsoft 365, and security

**Answer:** D

#### NEW QUESTION 207

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.

## Domains

+ Add domain Buy domain Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	Healthy	
<input type="checkbox"/> contoso.com	Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	No services selected	

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE; Each correct selection is worth one point.

Answer Area

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

### NEW QUESTION 209

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune. You plan to use Endpoint analytics to identify hardware issues. You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

- A. Configure the Endpoint analytics baseline regression threshold.
- B. Create a configuration profile.
- C. Create a Windows 10 Security Baseline profile
- D. Create a compliance policy.

Answer: B

### NEW QUESTION 210

HOTSPOT - (Topic 6)

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 Content Explorer Content viewer
Admin2	Security Administrator 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 215

- (Topic 6)

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

Name	Order	Created by	Last modified
Label1	0 - highest	Pri	04/24/2020
Label2	1	Pri	04/24/2020
Label3	0 - highest	Pri	04/24/2020
Label4	0 - highest	Pri	04/24/2020
Label5	5	Pri	04/24/2020
Label6	0 - highest	Pri	04/24/2020

Which labels can users apply to content?

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

Answer: C

## NEW QUESTION 220

HOTSPOT - (Topic 6)

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	Not applicable

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computer1



computer1

## Device summary

Risk level ⓘ

None

## Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

### Answer Area

Computer1 will be a member of [answer choice].

Group3 only  
Group4 only  
Group3 and Group4 only  
Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

Group1 only  
Group1 and Group2 only  
Group1, Group2, Group3, and Group4  
Ungrouped devices

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

Box 1: Group3 and Group4 only Computer1 has no Demo Tag.

Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

### NEW QUESTION 223

- (Topic 6)

You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

**Labels**

Label policies

Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label    Publish labels    Refresh

Name ↑	Order	Created by	Last modified
Label1	... 0-highest	Prvi	04/24/2020
– Label2	... 1	Prvi	04/24/2020
Label3	... 0-highest	Prvi	04/24/2020
Label4	... 0-highest	Prvi	04/24/2020
– Label5	... 5	Prvi	04/24/2020
Label6	0-highest	Prvi	04/24/2020

Which labels can users apply to content?

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

**Answer: D**

**Explanation:**

Reference:

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

#### NEW QUESTION 227

- (Topic 6)

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-628bec99-476a-2c13-5296-9dd081cdd808>

#### NEW QUESTION 229

HOTSPOT - (Topic 6)

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

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
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 234

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:

- Create a sensitive info type named SIT1 based on a regular expression.
- Add a watermark to all new documents that are matched by SIT1.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area



### NEW QUESTION 237

HOTSPOT - (Topic 6)

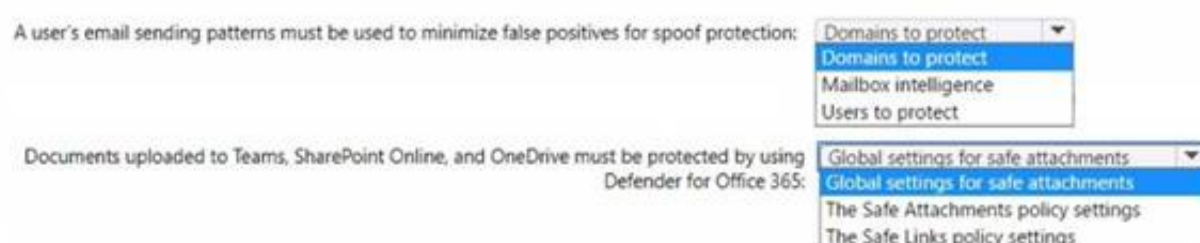
You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- A user's email sending patterns must be used to minimize false positives for spoof protection.
- Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.

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

#### Answer Area

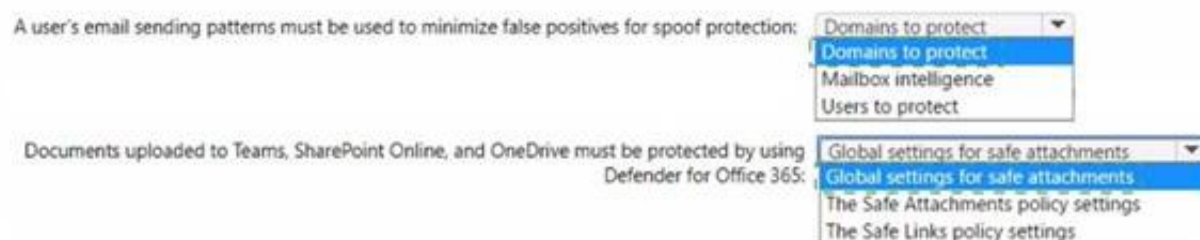


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



#### NEW QUESTION 241

- (Topic 6)

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:

? Password Hash Sync: Enabled

? Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

- A. none
- B. Used only1
- C. User1 and User2 only
- D. User1. User2, and User3

**Answer:** D

**Explanation:**

Reference:

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

#### NEW QUESTION 246

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

- A. a retention policy
- B. a retention label policy
- C. an auto-labeling policy
- D. an insider risk policy

**Answer:** C

**Explanation:**

Reference:

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

#### NEW QUESTION 250

- (Topic 6)

: 241

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 255

- (Topic 6)

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.

What should you use?

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

**Answer: C**

**Explanation:**

Reference:

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

#### NEW QUESTION 260

- (Topic 6)

You have a Microsoft 365 E5 tenant. Users store data in the following locations:

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

You need to retain Microsoft 365 data for two years.

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

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

**Answer: C**

**Explanation:**

Reference:

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

#### NEW QUESTION 263

- (Topic 6)

You have a Microsoft 365 E5 tenant. You configure sensitivity labels.

Users report that the Sensitivity button is unavailable in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

- A. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
- B. Publish the sensitivity labels.
- C. Create an auto-labeling policy
- D. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

**Answer: B**

#### NEW QUESTION 268

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

- ? Block emails that contain financial data.
- ? Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

- ? Use the following location: Exchange email.
- ? Display the following policy tip text: Message contains sensitive data.
- ? When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Results	Answer Area
The email will be blocked, and the user will receive the policy tip: Message blocked.	When the user sends an email that contains financial data and health records: <div>Result</div>
The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.	When the user sends an email that contains only financial data: <div>Result</div>
The email will be allowed, and the user will receive the policy tip: Message blocked.	
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.	
The email will be allowed, and a message policy tip will NOT be displayed.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

**NEW QUESTION 273**

- (Topic 6)

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 Update & Security to view the update history. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 277**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Sender is condition:

- ☒ DLP1 only
- ☐ DLP2 only
- ☐ DLP3 only
- ☐ DLP2 and DLP3 only
- ☐ DLP1, DLP2, and DLP3

File extension is condition:

- ☒ DLP1, DLP2, and DLP3
- ☐ DLP1 only
- ☐ DLP2 only
- ☐ DLP3 only
- ☐ DLP2 and DLP3 only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Sender is condition:

DLP1 only

DLP1 only

DLP2 only

DLP3 only

DLP2 and DLP3 only

DLP1, DLP2, and DLP3

File extension is condition:

DLP1, DLP2, and DLP3

DLP1 only

DLP2 only

DLP3 only


DLP2 and DLP3 only

DLP1, DLP2, and DLP3

NEW QUESTION 279


HOTSPOT - (Topic 6)

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



Group1

Private group • 1 owner • 1 member



General

Members

Settings

Microsoft Teams

General settings

☐ Allow external senders to email this group

☒ Send copies of group conversations and events to group members

☐ Hide from my organization's global address list

Privacy

☒ Private

☐ Public

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](https://entra.microsoft.com) from Microsoft 365 in place of the Azure AD admin center ([aad.portal.azure.com](https://aad.portal.azure.com)).

### NEW QUESTION 282

- (Topic 6)

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 Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

- A. Yes  
 B. No

**Answer:** B

### Explanation:

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

### NEW QUESTION 286

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).

You need to create a detection exclusion in Azure ATP. Which tool should you use?

- A. the Security & Compliance admin center  
 B. Microsoft Defender Security Center  
 C. the Microsoft 365 admin center  
 D. the Azure Advanced Threat Protection portal  
 E. the Cloud App Security portal

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is> <https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections>

#### NEW QUESTION 290

HOTSPOT - (Topic 6)

Your network contains an Active Directory domain and an Azure AD tenant.

You implement directory synchronization for all 10,000 users in the organization. You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

Which command should you run? To answer, select the appropriate options in the answer area.

**Answer Area**

Start-ADSyncSyncCycle	-PolicyType	Delta
Start-ADSyncSyncCycle		Delta
Set-ADSyncScheduler		Initial
Invoke-ADSyncRunProfile		Full

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Start-ADSyncSyncCycle	-PolicyType	Delta
Start-ADSyncSyncCycle		Delta
Set-ADSyncScheduler		Initial
Invoke-ADSyncRunProfile		Full

#### NEW QUESTION 294

- (Topic 6)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers

followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
- B. a sensitivity label
- C. a supervision policy
- D. a retention label

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

#### NEW QUESTION 295

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain

Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

**Answer:** A

**Explanation:**

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

? From the Security & Compliance tab of your browser, click Home.

? Click Data loss prevention > Policy.

? Click + Create a policy.  
? In Start with a template or create a custom policy, click Custom > Custom policy > Next.  
? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens  
? Etc.  
Reference:  
<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

NEW QUESTION 297

- (Topic 6)  
You have a Microsoft 365 E5 subscription.  
You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. End point analytics
- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

Answer: D

NEW QUESTION 298

HOTSPOT - (Topic 6)  
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:	<div><div>Configure hybrid Azure AD join.</div><div>Enable device writeback.</div><div>Enable password hash synchronization.</div></div>
To configure the domain:	<div><div>Add an alternative UPN suffix.</div><div>Register a service connection point.</div><div>Register a service principal name (SPN).</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 299

HOTSPOT - (Topic 6)  
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:  
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.  
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Solutions

 Catalog

 Audit

 Content search

 Communication compliance

 Data loss prevention

 eDiscovery

▼

 Data lifecycle management

 Information protection

 Information barriers

▼

 Insider risk management

 Records management

 Priva Privacy Risk Managem...

▼

 Priva Subject Rights Requests

 Settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology.

Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

- \* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
- \* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
- \* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
- \* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
- \* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

NEW QUESTION 300

- (Topic 6)

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. What permission should you assign to User1?

- A. the Information Protection administrator role from the Azure Active Directory admin center.
- B. the eDiscovery Manager role from the Microsoft 365 compliance center.
- C. the Compliance Management role from the Exchange admin center.
- D. the User management administrator role from the Microsoft 365 admin center.

**Answer: B**

#### NEW QUESTION 304

- (Topic 6)

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

You plan to implement insider risk management.

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

? Review alerts.

? Manage cases.

? Create notice templates.

? Review user emails by using Content explorer.

The solution must use the principle of least privilege. To which role group should you add User1?

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

**Answer: C**

#### Explanation:

Reference:

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

#### NEW QUESTION 305

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings.

Password write back is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.

The Azure AD password policy is configured as shown in the following exhibit. Password policy

Set the password policy for all users in your organization. Days before passwords expire 90

Days before a user is notified about 14 expiration

You confirm that User1 is synced to Azure AD.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 310

HOTSPOT - (Topic 6)

You work at a company named Contoso, Ltd.  
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.  
Contoso purchases a company named Fabrikam, Inc.  
Contoso plans to add the following domains to the Microsoft 365 subscription:

- fabrikam.com
- east.fabrikam.com
- west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.  
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Domains:

3

1

2

3

Enterpriseregistration DNS records:

3

1

2

3

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Domains:

3

1

2

3

Enterpriseregistration DNS records:

3

1

2

3

NEW QUESTION 311

HOTSPOT - (Topic 6)

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:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input checked="" type="radio"/>	<input type="radio"/>

## NEW QUESTION 312

- (Topic 6)

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.

Users in other departments must not be restricted.

What should you do?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the safe links policy Global settings.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

Answer: D

Explanation:

Use the Microsoft 365 Defender portal to create Safe Links policies

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinks2.

\* 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.

\* 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

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

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

Users: The specified mailboxes, mail users, or mail contacts.

\*-> Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).  
 The specified Microsoft 365 Groups.  
 Domains: All recipients in the specified accepted domains in your organization. Etc.  
 Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>

#### NEW QUESTION 314

HOTSPOT - (Topic 6)

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:

<input type="checkbox"/>	Credential harvest
<input type="checkbox"/>	Link to malware
<input type="checkbox"/>	Malware attachment

Training experience:

<input type="checkbox"/>	Identity Theft
<input type="checkbox"/>	Mass Market Phishing
<input type="checkbox"/>	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

#### NEW QUESTION 315

- (Topic 6)

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.

⬇ Export12 items🔍 Search🔼 Filter☰ Group by

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 316

HOTSPOT - (Topic 6)

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

Users may register their devices with Azure AD ⓘ  

AllNone

Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ  

YesNo

Maximum number of devices per user ⓘ  

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).  
For each of the following statement, select Yes if the statement is true. Otherwise, select No.  
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 can enroll all the devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll all the devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 319

- (Topic 6)

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

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION 322

HOTSPOT - (Topic 6)

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	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	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.

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 327

HOTSPOT - (Topic 6)

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

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

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.  
You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.  
Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

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

Users who can assign Retention2:

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

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Users who can assign Retention1:

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

Users who can assign Retention2:

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

#### NEW QUESTION 329

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to configure policies to meet the following requirements:

? Customize the common attachments filter.

? Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

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

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Anti-malware

Customize the common attachments filter. See step 5 below.

\* 1. Use the Microsoft 365 Defender portal to create anti-malware policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use <https://security.microsoft.com/antimalwarev2>

\* 2. On the Anti-malware page, select Create to open the new anti-malware policy wizard. On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.

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

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

\* 5. On the Protection settings page, configure the following settings: Protection settings section:

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

\* 6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains. Anti-phishing policies in Microsoft 365

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

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

### NEW QUESTION 332

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

- A. From the Cloud App Security admin center, select Users and accounts.
- B. From the Microsoft 365 security center, view the Threat tracker.
- C. From the Microsoft 365 admin center, view the Security & compliance report.
- D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

### NEW QUESTION 336

- (Topic 6)

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?

- A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile
- B. Assign the profile to all the computer
- C. Instruct users to restart their computer and perform a network restart.
- D. Enroll the computers in Microsoft Intun
- E. Create a configuration profile by using the Edition upgrade and mode switch templat
- F. From the Microsoft Endpoint Manager admincenter, assign the profile to all the computers and instruct users to restart their computer.
- G. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
- H. Instruct users to run the provisioning package from SharePoint Online.
- I. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
- J. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

### NEW QUESTION 338

HOTSPOT - (Topic 6)

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

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

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

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input type="radio"/>
User3 can assign licenses to User1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can assign licenses to User1.	<input checked="" type="radio"/>	<input type="radio"/>

### NEW QUESTION 340

HOTSPOT - (Topic 5)

You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

Admin1 and Admin3 only

Admin1 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and Admin4

Blade:

Service Health

Reports

Service Health

Message center

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

## Answer Area

Users:

Blade:

### NEW QUESTION 344

- (Topic 5)

You need to configure just in time access to meet the technical requirements. What should you use?

- A. entitlement management
- B. Azure AD Privileged Identity Management (PIM)
- C. access reviews
- D. Azure AD Identity Protection

**Answer: B**

### NEW QUESTION 347

- (Topic 5)

You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs. What should you do?

- A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
- B. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.
- C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
- D. From the Microsoft Azure AD Connect wizard, select Manage federation.

**Answer: A**

### NEW QUESTION 352

- (Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. alias (CNAME)

**Answer: D**

#### Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

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

Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider>

### NEW QUESTION 356

- (Topic 4)

Which role should you assign to User1?

Available Choices (select all choices that are correct)

- A. Hygiene Management
- B. Security Reader
- C. Security Administrator

D. Records Management

**Answer:** C

**Explanation:**

A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.

Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

**NEW QUESTION 357**

HOTSPOT - (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:**

Role group:

▼
Reviewer
Global reader
Data Investigator
Compliance Management

Tool:

▼
Exchange admin center
SharePoint admin center
Microsoft 365 admin center
Microsoft 365 security center

**NEW QUESTION 360**

- (Topic 3)

You need to configure Office on the web to meet the technical requirements. What should you do?

- A. Assign the Global reader role to User1.
- B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
- C. Configure an auto-labeling policy to apply the sensitivity labels.
- D. Assign the Office apps admin role to User1.

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 362

- (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/safe-attachments.md>

#### NEW QUESTION 367

- (Topic 2)

You need to meet the technical requirement for large-volume document retrieval. What should you create?

- A. a data loss prevention (DLP) policy from the Security & Compliance admin center
- B. an alert policy from the Security & Compliance admin center
- C. a file policy from Microsoft Cloud App Security
- D. an activity policy from Microsoft Cloud App Security

**Answer: D**

#### Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts>

#### NEW QUESTION 372

HOTSPOT - (Topic 1)

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Seattle:

<input type="checkbox"/>
6 months
18 months
24 months
30 months
5 years

New York:

<input type="checkbox"/>
6 months
18 months
24 months
30 months
5 years

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date

References:

<https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>

#### NEW QUESTION 376

HOTSPOT - (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:**

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

#### NEW QUESTION 378

- (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 380

- (Topic 6)

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- A. the status of the DLP policy
- B. the user overrides of the DLP policy rule
- C. the locations of the DLP policy
- D. the conditions of the DLP policy rule

**Answer:** D

#### NEW QUESTION 381

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. a sensitive info type
- C. a data loss prevention (DLP) policy
- D. a sensitivity label
- E. a retention label
- F. a retention label policy

**Answer:** CE

**NEW QUESTION 383**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

## How do you want the alert to be triggered?

- ☐ Every time an activity matches the rule
- ☐ When the volume of matched activities reaches a threshold

More than or equal to  activities

During the last  minutes

On

- ☒ When the volume of matched activities becomes unusual

On

You need to identify the following:

? How many days it will take to establish a baseline for unusual activity.

? Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

How many days it will take to establish the baseline:


Whether the alerts will be triggered during the establishment of the baseline:


A. Mastered

B. Not Mastered

**Answer: A**

**Explanation:**

How many days it will take to establish the baseline:


Whether the alerts will be triggered during the establishment of the baseline:

#### NEW QUESTION 384

HOTSPOT - (Topic 6)

HOTSPOT

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

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

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Groups that can be restored:

▼

Group3 only

Group1 and Group2 only

Group2 and Group4 only

Group1, Group2, and Group3 only

Group1, Group2, Group3, and Group4

Retention period:

▼

24 hours

7 days

14 days

30 days

90 days

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Group3 only

Box 2: 30 days

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

#### NEW QUESTION 386

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

- A. Microsoft Defender for CloudUse the
- B. Microsoft Purview
- C. Azure Arc
- D. Microsoft Defender for Identity

**Answer:** D

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

#### NEW QUESTION 387

- (Topic 6)

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 392**

- (Topic 6)

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-628bec99-476a-2c13-5296-9dd081cdd808>

**NEW QUESTION 397**

- (Topic 6)

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

You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

What should you do?

- A. Create a new Anti-malware policy
- B. Configure the Safe Links global settings.
- C. Create a new Anti-phishing policy
- D. Configure the Safe Attachments global settings.

**Answer:** D

**Explanation:**

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint,

OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about>

**NEW QUESTION 398**

HOTSPOT - (Topic 6)

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

Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1:

None of the groups

None of the groups

Group2 only

Group2 and Group4 only

Group2, Group4, Group5, and Group6 only

Group2, Group3, Group4, Group5, and Group6

Group4:

Group5 only

None of the groups

Group5 only

Group3 and Group5 only

Group1, Group2, Group3, and Group5 only

Group1, Group2, Group3, Group5, and Group6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Group1:

None of the groups

None of the groups

Group2 only

Group2 and Group4 only

Group2, Group4, Group5, and Group6 only

Group2, Group3, Group4, Group5, and Group6

Group4:

Group5 only

None of the groups

Group5 only

Group3 and Group5 only

Group1, Group2, Group3, and Group5 only

Group1, Group2, Group3, Group5, and Group6

NEW QUESTION 400

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents. What should you use?

- A. a custom detection rule
- B. a threat policy
- C. an alert policy
- D. a notification rule

Answer: C

NEW QUESTION 401

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

<https://www.2passeasy.com/dumps/MS-102/>

## Money Back Guarantee

### 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 FirstTry
- \* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year