

# Exam Questions MS-102

Microsoft 365 Administrator Exam

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



NEW QUESTION 1

DRAG DROP - (Topic 6)  
DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.  
You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	<ul style="list-style-type: none"><li>Manage service requests.</li><li>Purchase new services.</li><li>Manage subscriptions.</li><li>Monitor service health.</li></ul>
Group2	<ul style="list-style-type: none"><li>Assign licenses.</li><li>Add users and groups.</li><li>Create and manage user views.</li><li>Update password expiration policies.</li></ul>

The solution must use the principle of least privilege.  
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1: 

Role

Group2: 

Role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Box 1: Billing admin manage service request Purchase new services Etc.  
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.  
Box 2: User admin User admin  
Assign the User admin role to users who need to do the following for all users:  
- Add users and groups  
- Assign licenses  
- Manage most users properties  
- Create and manage user views  
- Update password expiration policies  
- Manage service requests  
- Monitor service health

NEW QUESTION 2

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:

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Recent Microsoft service issues:

Microsoft Secure Score

Adoption Score

Service health

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 3

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	Answer Area
Create a sensitivity label.	Create a sensitivity label.
Create an auto-labeling policy.	
Create a sensitive information type.	Publish the label.
Wait 24 hours, and then turn on the policy.	
Publish the label.	Create an auto-labeling policy.
Create a retention label.	
Wait eight hours, and then turn on the policy.	

NEW QUESTION 4

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:

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password

Require multi-factor authentication

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 5

- (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 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

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 6

- (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 7**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:

? Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).

? Report on shared documents that contain PII.

What should you create?

A. an alert policy

B. a data loss prevention (DLP) policy

C. a retention policy

D. a Microsoft Cloud App Security policy

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

**NEW QUESTION 8**

- (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 9**

- (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 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 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 10

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.  
 Which objects will sync to Azure AD?

- A. Group1 only
- B. User1 and User2 only
- C. Group1 and User1 only
- D. Group1, User1, and User2

**Answer: D**

**Explanation:**

Disabled accounts  
 Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.  
 The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts>

#### NEW QUESTION 12

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.  
 What should you identify? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

## Answer Area

Microsoft 365 setting:

Office installation options
Privileged access
Release preferences

User:

User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

## Answer Area

Microsoft 365 setting:

Office installation options
Privileged access
Release preferences

User:

User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only

### NEW QUESTION 16

- (Topic 6)

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

- A. conditional access  
 B. account protection  
 C. attack surface reduction (ASR)  
 D. Endpoint detection and response

Answer: A

Explanation:

Reference:

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

### NEW QUESTION 19

- (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 24

- (Topic 6)

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

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

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

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile>

<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

#### NEW QUESTION 29

- (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 SharePoint Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 33

- (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 38

- (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 43

- (Topic 6)

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

**Answer:** A

### NEW QUESTION 46

- (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 50

- (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 55

HOTSPOT - (Topic 6)

Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

You need to identify which users can perform the following administrative tasks:

- Reset the password of User4.
- Modify the value for the manager attribute of User4.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Reset the password of User4: User1 and User3 only

- User1 only
- User2 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

Modify the value for the manager attribute of User4: User3 only

- User2 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Answer Area

Reset the password of User4:

Modify the value for the manager attribute of User4:

NEW QUESTION 57

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 60

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1. You plan to use Mailbox1 to collect and analyze unfiltered email messages. You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1. What should you do?

- A. Configure a retention policy for Mailbox1.  
 B. Create a mail flow rule.  
 C. Configure Mailbox1 as a SecOps mailbox.  
 D. Place a litigation hold on Mailbox1.

**Answer:** D

#### NEW QUESTION 61

- (Topic 6)

You have a Microsoft 365 F5 subscription. You plan to deploy 100 new Windows 10 devices. You need to order the appropriate version of Windows 10 for the new devices. The version must Meet the following requirements.  
 Be serviced for a minimum of 24 months.  
 Support Microsoft Application Virtualization (App-V) Which version should you identify?

- A. Window 10 Pro, version 1909  
 B. Window 10 Pro, version 2004  
 C. Window 10 Pro, version 1909  
 D. Window 10 Enterprise, version 2004

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/windows/release-health/release-information>

<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations>

#### NEW QUESTION 63

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

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

- ? Users or workload identities assignments: All users
- ? Cloud apps or actions assignment: App1
- ? Conditions: Include all trusted locations
- ? Grant access: Require multi-factor authentication

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
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes  
\* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1’s MFA status is disabled. The MFA requirement in the conditional access policy will override the user’s MFA status of disabled. Therefore, User1 must use MFA.  
Box 2: Yes.  
\* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.  
Box 3: No.  
IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

NEW QUESTION 67

- (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 72

HOTSPOT - (Topic 6)  
HOTSPOT  
You have a Microsoft 365 E5 subscription.  
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

A user that is assigned the Global Administrator role as active [answer choice].

will lose the role after eight hours

can reactivate the role every eight hours

can reactivate the role every 15 days

will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

for up to eight hours

for up to three months

for up to 15 days

until the requests are revoked manually

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: will lose the role after eight hours  
 From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)  
 Box 2: for up to three months  
 We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 76

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☒☐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)☐☐

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 79

- (Topic 6)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

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

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

Solutions: You instruct User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

### NEW QUESTION 83

DRAG DROP - (Topic 6)

Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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.

#### Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

#### Answer Area

Company-owned devices:

Solution

Personal devices:

Solution

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

#### Answer Area

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy

### NEW QUESTION 84

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

NEW QUESTION 88

HOTSPOT - (Topic 6)

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

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
- The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status  
Mailflow status report  
Spoof detections  
Threat protection status  
URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report  
Mailflow status report  
Spoof detections  
Threat protection status  
URL threat protection

NEW QUESTION 90

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 94

- (Topic 6)

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You need to prevent the members of Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.

What should you use?

- A. information barriers
- B. communication compliance policies
- C. moderated distribution groups
- D. administrator units in Azure Active Directory (Azure AD)

**Answer:** A

#### NEW QUESTION 96

- (Topic 6)

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

- A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
- B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
- C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
- D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

**Answer:** A

#### Explanation:

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

#### NEW QUESTION 101

- (Topic 6)

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

- A. 1 day
- B. 7 days
- C. 30 days
- D. 90 days

**Answer:** C

#### Explanation:

View email security reports in the Microsoft 365 Defender portal

The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security>

#### NEW QUESTION 103

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 users](#) [Add groups](#) [Upload users](#) ... [Filter](#)

<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 users](#) [Add 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.

Answer Area

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:

Answer Area

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 104

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	Not applicable
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD)

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
 NOTE: Each correct selection is worth one point.

**Actions**  

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

**Answer Area**

Device1: 

Action

Device2: 

Action

Device3: 

Action

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**  

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

**Answer Area**

Device1: 

Disable BitLocker.

Device2: 

Switch to UEFI.

Device3: 

Upgrade to Windows 10 Enterprise.

### NEW QUESTION 105

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 110

- (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 113

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

The device limit restrictions in Endpoint manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

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

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 114

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☐

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐
☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes

Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

#### NEW QUESTION 115

- (Topic 6)

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager. Devices are onboarded by using Microsoft Defender for Endpoint. You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint. What should you create first?

- A. a device configuration policy
- B. a device compliance policy
- C. a conditional access policy
- D. an endpoint detection and response policy

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 116**

- (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 117**

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to meet the following requirements:

- Report a Microsoft 365 service issue.
- Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: <input type="text"/>
New service request	To request help on how to add a new user to the tenant: <input type="text"/>
Product feedback	
Service health	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: New service request
New service request	To request help on how to add a new user to the tenant: Message center
Product feedback	
Service health	

**NEW QUESTION 118**

- (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 named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

## USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD. Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

### Explanation:

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

## NEW QUESTION 119

- (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 122

- (Topic 6)

You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

- A. Admin2, Admin3, and Admin4 only
- B. Admin1, Admin2, Admin3, and Admin4
- C. Admin2 and Admin3 only
- D. Admin3 only
- E. Admin1 and Admin3 only

**Answer:** E

**Explanation:**

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

**NEW QUESTION 124**

- (Topic 6)

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

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:

? To all users, deploy an Office 365 E3 license without the Power Automate license option.

? To all users, deploy an Enterprise Mobility + Security E5 license.

? To the users in the research department only, deploy a Power BI Pro license.

? To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

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

**Answer:** C

**Explanation:**

One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

<https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-more>

**NEW QUESTION 128**

- (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 133

HOTSPOT - (Topic 6)

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

Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

You onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in The answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Computer1:

Computer2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Answer Area

Computer1:

Computer2:

### NEW QUESTION 138

- (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 143

- (Topic 6)

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

- A. 1
- B. 2
- C. 5
- D. 10

Answer: C

#### Explanation:

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq>

#### NEW QUESTION 144

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

#### Answer Area

Tool:

<input type="checkbox"/> AccessChk
<input type="checkbox"/> Azure AD Connect
<input type="checkbox"/> Active Directory Explorer
<input type="checkbox"/> IdFix

Required group membership:

<input type="checkbox"/> Domain Admins
<input type="checkbox"/> Domain Users
<input type="checkbox"/> Server Operators
<input type="checkbox"/> Enterprise Admins

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Windows Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

\* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

The user account that you use to run IdFix must have read and write access to the AD DS domain.

If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.

\* Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

Incorrect:

\* Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

\* Server Operator

Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.

\* Domain Users - too few permissions

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

#### NEW QUESTION 146

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings: 1.Assignments

? Users or workload identities: Group1

? Cloud apps or actions: Office 365 SharePoint Online

? Conditions

- Filter for devices: Exclude filtered devices from the policy

- Rule syntax: device.displayName -startsWith "Device" 2.Access controls

? Grant

- Grant: Block access

? Session: 0 controls selected 3.Enable policy: On

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 Site1 from Device1.

☐
☐

User2 can access Site1 from Device2.

☐
☐

User2 can access Site1 from Device3.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

#### Explanation:

Box 1: No

User1 is member of Group1 and has Device1.

Device1 is not Azure AD joined.

Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.

Box 2: Yes

User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.

Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes

User2 is member of Group1 and has devices Device2 and Device3.

Device3 is Android and is Azure AD registered.

Device3 is excluded from CAPolicy1 (which would block access to Site1).

Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

#### NEW QUESTION 150

- (Topic 6)

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

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

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

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 151

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ ☒ Yes ☐ No

Custom banned password list ⓘ

3hundred

Eleven

Falcon

Project

Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ ☒ Yes ☐ No

Mode ⓘ ☒ Enforced ☐ Audit

User1 attempts to update their password to the following passwords:

? F@lcon

? Project22

? T4il\$pin45dg4

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

[Answer choice] will be accepted as a password.

▼

Only T4il\$pin45dg4

Only F@lcon and T4il\$pin45dg4

Only Project22 and T4il\$pin45dg4

F@lcon, Project22, and T4il\$pin45dg4

▼

will be locked out

will trigger a user risk

can attempt to sign in again immediately

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Box 1: Only T4il\$pin45dg4

Box 2: can attempt to sign in immediately Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

- ? Sign in to the Entra portal.
- ? Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
- ? Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
- ? The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
- ? Set the Lockout duration in seconds, to the length in seconds of each lockout.
- ? The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

### NEW QUESTION 152

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a user named User1 You create a retention label named Retention1 that is published to all locations.

You need to ensure that User1 can label email messages by using Retention1 as soon as possible.

Which cmdlet should you run in Microsoft Exchange Online PowerShell?

- A. Start-MpScan
- B. Start-Process
- C. Start-ManagedFolderAsslstant
- D. Start-AppBackgroundTask

**Answer:** C

### NEW QUESTION 157

- (Topic 6)

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

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

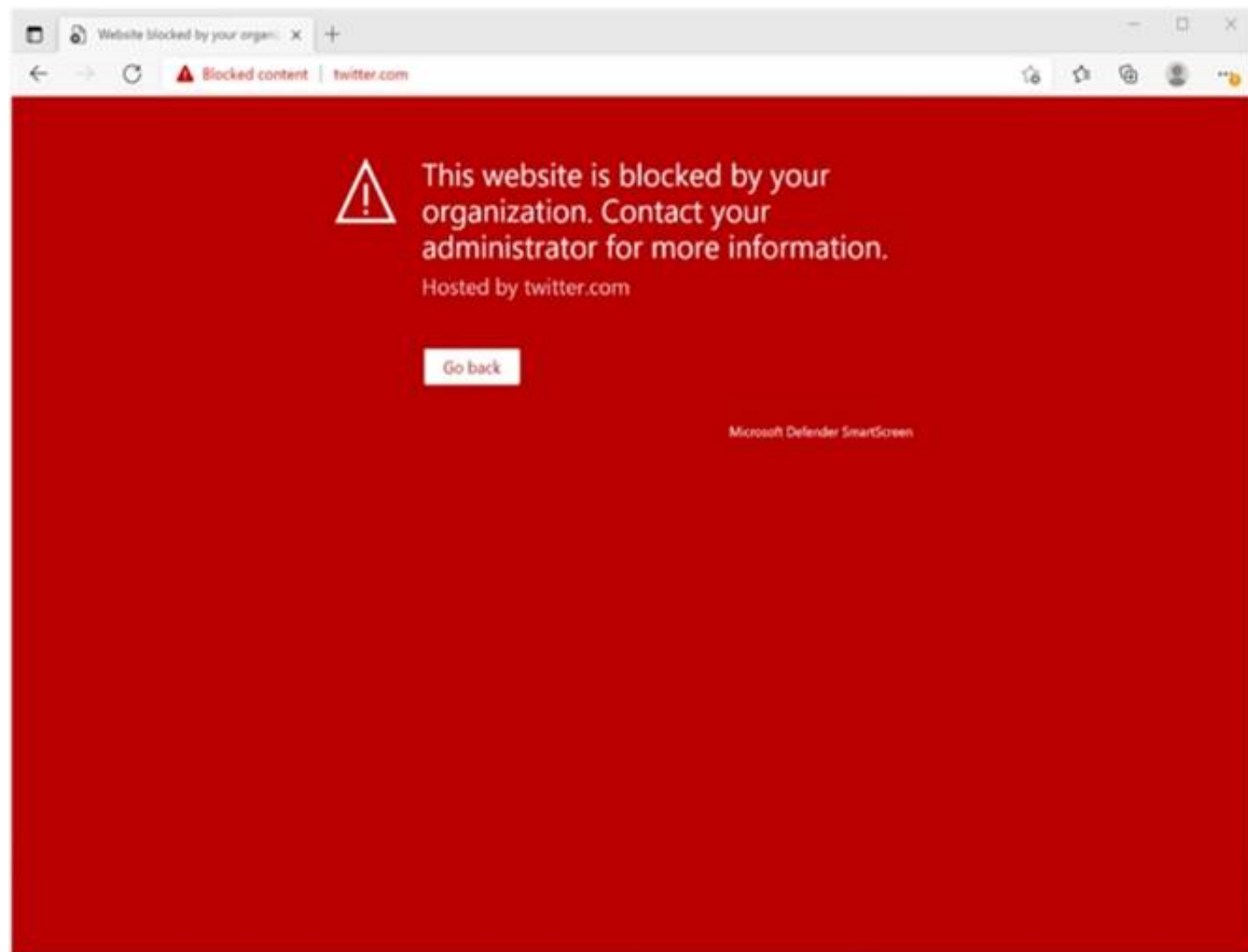


You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

**Answer:** E

### Explanation:



#### This Website Is Blocked By Your Organization

Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.

Reference: <https://jadexstrategic.com/web-protection/>

#### NEW QUESTION 159

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

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

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

Enable policy

Report-only On Off

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.

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

Enable policy  
Report-only On Off ✓

⚠ 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.

NEW QUESTION 161

- (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 162

- (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 167

- (Topic 6)

You have a Microsoft 365 subscription that uses Security & Compliance retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

- A. Add locations to the policy
- B. Reduce the duration of policy
- C. Remove locations from the policy

- D. Extend the duration of the policy
- E. Disable the policy

**Answer:** AB

#### NEW QUESTION 168

- (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 pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 170

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a data loss prevention (DLP) policy
- B. a sensitivity label policy
- C. a Microsoft Cloud App Security file policy
- D. a communication compliance policy
- E. a retention label policy

**Answer:** AD

#### NEW QUESTION 172

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

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

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

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

**Answer:** C

#### Explanation:

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

Reference:

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

#### NEW QUESTION 176

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: DevtceGroup1, 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	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input checked="" type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input checked="" type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 178

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

- ? Scope type: Directory
- ? Selected members: Group1

? Assignment type: Active  
? Assignment starts: Mar 15, 2023  
? Assignment ends: Aug 15, 2023  
You add the following assignment for the Exchange Administrator role:  
? Scope type: Directory  
? Selected members: Group2  
? Assignment type: Eligible  
? Assignment starts: Jun 15, 2023  
? Assignment ends: Oct 15, 2023

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

NOTE: Each correct selection is worth one point.

#### Answer Area

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

- A. Mastered  
B. Not Mastered

Answer: A

#### Explanation:

Box 1: Yes

Admin1 is member of Group1.

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

July 15, 2023 is with the assignment period.

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

Box 2: No

Admin2 is member of Group2.

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

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

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

Box 3: Yes

Admin3 is member of Group1 and Group2.

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

May 1, 2023 is with the assignment period.

#### NEW QUESTION 179

DRAG DROP - (Topic 6)

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

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune- managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method 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.

Onboarding method	Device Type
A local script	Corporate: <input type="text"/>
Group Policy	BYOD: <input type="text"/>
Integration with Microsoft Defender for Cloud	
Microsoft Intune	
Virtual Desktop Infrastructure (VDI) scripts	

- A. Mastered  
B. Not Mastered

Answer: A

#### Explanation:

Onboarding method

A local script

Group Policy

Integration with Microsoft Defender for Cloud

Microsoft Intune

Virtual Desktop Infrastructure (VDI) scripts

Device Type

Corporate: 

Microsoft Intune

BYOD: 

Integration with Microsoft Defender for Cloud

NEW QUESTION 181

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)	<div></div> Healthy	
<input type="checkbox"/> contoso.com	<div></div> Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	<div></div> 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].

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

NEW QUESTION 185

- (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 189

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 193

HOTSPOT - (Topic 6)

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

You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

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

Answer Area

Portal:

Microsoft 365 Defender portal

Microsoft 365 admin center

Microsoft 365 Defender portal

Microsoft Purview compliance portal

Feature:

Configuration analyzer

Configuration analyzer

Preset security policies

Threat tracker

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

Portal:

Feature:

NEW QUESTION 196

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 199

- (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 203

- (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 206**

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization. To which users can User1 send documents that contain PII?

- A. User2only
- B. User2and User3only
- C. User2, User3, and User4 only
- D. User2, User3, User4, and User5

**Answer:** B

**NEW QUESTION 208**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

? Block a vulnerable app until the app is updated.

? Block an application executable based on a file hash.

The solution must minimize administrative effort.

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**

Block a vulnerable app until the app is updated:

An allow or block file

A file indicator

A remediation request

An update ring

Block an application executable based on a file hash:

An allow or block file

A file indicator

A remediation request

An update ring

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

? Select a security recommendation to see a flyout with more information.

? Select Request remediation.

? Select whether you want to apply the remediation and mitigation to all device groups or only a few.

? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

? Pick a Remediation due date and select Next.

? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.

? Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

### NEW QUESTION 210

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 215

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.

From Azure AD Identity Protection, you enable a sign-in risk policy.

Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.

What should you configure?

- A. the Tenant restrictions settings in Azure AD  
B. a trusted location  
C. a Conditional Access policy exclusion  
D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:

There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to

self-remediate when risk is detected:

Sign-in risk policy User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

### NEW QUESTION 218

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 user's email sending patterns must be used to minimize false positives for spoof protection:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

### NEW QUESTION 220

- (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. User1 only  
 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 225

- (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 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 Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### NEW QUESTION 230

- (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 233

- (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 234

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 tenant.

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

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

The screenshot shows a list of compliance solutions on the left and their corresponding DLP policies in the 'Answer Area' on the right.

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

### NEW QUESTION 236

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

### NEW QUESTION 239

- (Topic 6)

You have a Microsoft 365 subscription.

You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.

You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.

What should you modify?

- A. the policy rule exceptions  
 B. the DLP policy locations  
 C. the policy rule conditions  
 D. the policy rule actions

Answer: C

### NEW QUESTION 243

## HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices.

You need to ensure that the devices are marked as compliant.

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

NOTE: Each correct selection is worth one point.

### Answer Area

#### Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured

Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

A. Mastered

B. Not Mastered

Answer: A

### Explanation:

#### Answer Area

#### Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured

Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

## NEW QUESTION 248

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

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

Answer: C

### Explanation:

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

Specific types of sensitive information.

Specific keywords that match a query you create.

Pattern matches for a trainable classifier.

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

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels) Teams chats

Teams private channel messages Yammer community messages Yammer user messages

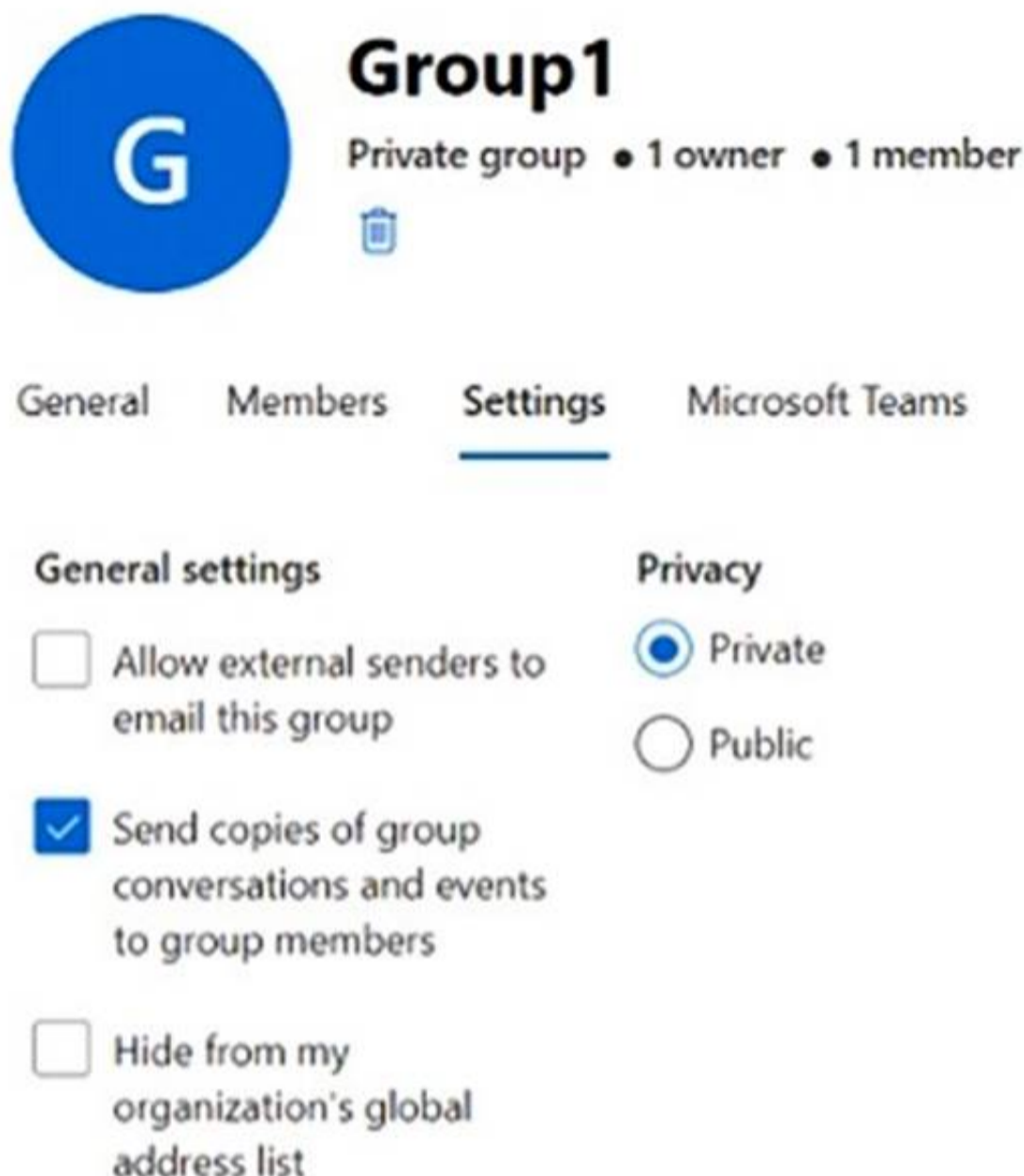
Reference:

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

### NEW QUESTION 253

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.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Action:

- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal:

- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to <https://admin.microsoft.com>. On the left pane, click on "Users", then click "Guest Users".

On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will

create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products

Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

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

#### NEW QUESTION 254

- (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 258

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

You create a retention label named Label 1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
  - Specifies the OneDrive accounts and SharePoint sites locations
- You run the following command.

Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention Strue -Force

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 add Exchange email as a location to Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can add the word Acquisition to Policy1.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

**Answer: A**

#### Explanation:

### Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>

### NEW QUESTION 259

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  
Start-ADSyncSyncCycle  
Set-ADSyncScheduler  
Invoke-ADSyncRunProfile

-PolicyType

Delta  
Delta  
Initial  
Full

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

### Answer Area

Start-ADSyncSyncCycle  
Start-ADSyncSyncCycle  
Set-ADSyncScheduler  
Invoke-ADSyncRunProfile

-PolicyType

Delta  
Delta  
Initial  
Full

### NEW QUESTION 261

- (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 262

- (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 263

- (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 266

HOTSPOT - (Topic 6)

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

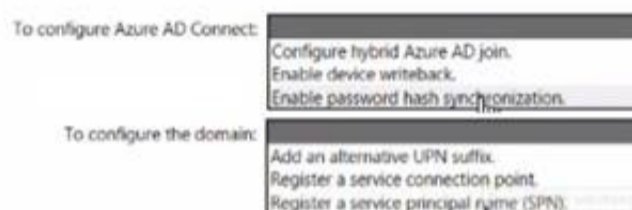
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

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

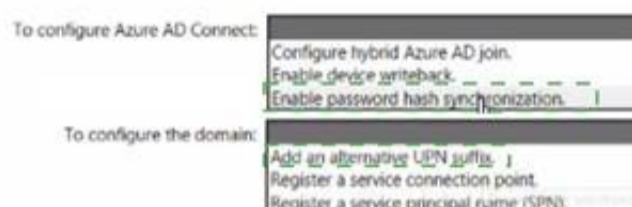


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area



### NEW QUESTION 270

- (Topic 6)

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

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

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

What should you include in the recommendation?

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

**Answer: D**

#### NEW QUESTION 272

- (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 274

- (Topic 6)

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.

Company policy requires that the devices have the following configurations:

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

You need to configure the devices to meet the requirements.

What should you use?

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

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 278

- (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 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 on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

## USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

### Explanation:

This is not a permissions issue.

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

## NEW QUESTION 287

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:

Credential harvest

Link to malware

Malware attachment

Training experience:

Identity Theft

Mass Market Phishing

Web Phishing

- A. Mastered
- B. Not Mastered

**Answer: A**

### Explanation:

Box 1: Credential Harvest

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

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

Credential Harvest Malware Attachment Link to Malware

Etc.

Box 2: Mass Market Phishing

#### NEW QUESTION 291

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

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

#### Answer Area

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

### Answer Area

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

### NEW QUESTION 296

- (Topic 6)

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

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

- A. Device 1, Device2, and Device3 only
- B. Device3 only
- C. Device2 and Device3 only
- D. Device1, Device2, Devices and Device4

**Answer:** C

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements>

### NEW QUESTION 299

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.

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

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

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

NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:

Device 1 only
Device 1 and Device 2 only
Device 1 and Device 3 only
Device 1 and Device 4 only
Device 1, Device 2, and Device 4 only
Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

A conditional access policy only
A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile, device compliance policy, and conditional access policy

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, table Description automatically generated with medium confidence

**NEW QUESTION 302**

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains the following user:

? Name: User1

? UPN: user1@contoso.com

? Email address: user1@marketing.contoso.com

? MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.

You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.

What should you do?

- A. Assign an MFA registration policy to User1.
- B. Reset the password of User1.
- C. Add an alternate email address for User1.
- D. Modify the UPN of User1.

**Answer:** D

**Explanation:**

Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

Reference:

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>

**NEW QUESTION 307**

- (Topic 6)

You have a Microsoft 365 subscription. You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.

You need to change the email address used to verify the domain. What should you do?

- A. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
- B. Add a TXT record to the DNS zone of the domain.
- C. From the domain registrar, modify the contact information of the domain.
- D. Modify the NS records for the domain.

**Answer:** C

**NEW QUESTION 311**

- (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 313

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 315

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

The default shared folder location for User1 is:

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

The default Office theme for User 2 is:

Colorful  
Dark Gray  
White

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins\_all\_users

https://sharepoint.contoso.com/addins\_office\_users

https://sharepoint.contoso.com/addins\_sales\_team\_users\_i

The default Office theme for User 2 is:

Colorful

Dark Gray

White

NEW QUESTION 318

- (Topic 6)  
You have a Microsoft 365 subscription.  
You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again. When will File1.docx be deleted automatically?

- A. January 1,2023
- B. January 1,2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

Answer: D

Explanation:

Retention wins over deletion. Note:  
Explanation for the four different principles:  
\* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system- initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.  
\* 2. Etc. Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

NEW QUESTION 323

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

Anti-malware

Anti-phishing

Anti-spam

Safe Attachments

Answer Area

Customize the common attachments filter:

Enable impersonation protection for sender domains:

- 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 327

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	None	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	None	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the 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
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
App3 can be installed automatically for UserGroup1.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input checked="" type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
App3 can be installed automatically for UserGroup1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 331

- (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 profil
- 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 332

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create retention label

Name

Retention settings

Finish

Review and finish

Name

Name

6Months

Edit

Retention settings

Retention period

6 months

Edit

Retention action

Retain and Delete

Edit

Based on

Based on when it was created

Edit

Back

Create label

Cancel

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

Passing Certification Exams Made Easy

visit - <https://www.2PassEasy.com>

Auto-labeling > Create auto-labeling policy

✓ Name

● Info to label

● Create content query

○ Scope

○ Label

○ Finish

### Apply label to content matching this query

Conditions

ProjectX

+ Add condition

?

Back

Next

Cancel

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Box 1: No  
Box 2: Yes  
Box 3: No

NEW QUESTION 334

.....

## 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