

## Exam Questions MS-102

Microsoft 365 Administrator Exam

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



**NEW QUESTION 1**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant

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

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

NOTE: Each correct selection is worth one point.

### Choose locations to apply the policy

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

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

### Choose locations to apply the policy

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

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

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

**NEW QUESTION 2**

HOTSPOT - (Topic 6)

**HOTSPOT**

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

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

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Install:  ▼

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

Server:  ▼

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

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

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

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

**NEW QUESTION 3**

- (Topic 6)

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

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

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

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

**Answer:** D

**Explanation:**

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

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

Reference:

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

**NEW QUESTION 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:

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

To enable self-remediation, select:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: A user risk policy

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

User risk-based Conditional Access policy

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

Block access

Allow access but require a secure password change.

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

Box 2: Require password change

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

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

#### NEW QUESTION 5

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

**Answer:** D

#### NEW QUESTION 6

- (Topic 6)

Your company has offices in five cities. The company has a Microsoft 365 tenant.

Each office is managed by a local administrator. You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in Intune that meets the following requirements:

? Local administrators must be able to manage only the resources in their respective office.

? Local administrators must be prevented from managing resources in other offices.

? Administrative effort must be minimized.

What should you include in the recommendation?

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

**Answer:** B

#### Explanation:

Reference:

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

#### 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 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing, outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security & Compliance admin center you create a threat management policy.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### NEW QUESTION 9

- (Topic 6)

Your company has 10,000 users who access all applications from an on-premises data center.

You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible. What should you do?

- A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
- B. Run idfix.exe, and then click Edit.
- C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
- D. Run idfix.exe, and then click Complete.

**Answer: B**

**Explanation:**

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix>

#### NEW QUESTION 10

- (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 12**

- (Topic 6)

Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score. You need to assign the following improvement action to User1:Enable self-service password reset. What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

**Answer: D**

**Explanation:**

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

**NEW QUESTION 16**

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1. Does this meet the goal?

- A. yes
- B. No

**Answer: A**

**NEW QUESTION 20**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Portal:

Group types:

Group types:

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

Portal:

Group types:

Group types:

**NEW QUESTION 23**

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:

User:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Microsoft 365 setting:

User:

**NEW QUESTION 27**

- (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 29**

- (Topic 6)

You have a Microsoft E5 subscription.

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

What should you implement?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 33**

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:  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

**NEW QUESTION 34**

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 38**

- (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 42**

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	None
User4	Password Administrator

External collaboration settings have default configuration.

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

- Modify the password protection policy.
- Create guest user accounts.

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**

Modify the password protection policy:  User1 only  
 User1 only  
 User1 and User2 only  
 User1, User2, and User4 only  
 User1, User2, User3, and User4

Create new guest users in Azure AD:  User1 and User2 only  
 User1 only  
 User1 and User2 only  
 User1, User2, and User4 only  
 User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Modify the password protection policy:  User1 only  
 User1 only  
 User1 and User2 only  
 User1, User2, and User4 only  
 User1, User2, User3, and User4

Create new guest users in Azure AD:  User1 and User2 only  
 User1 only  
 User1 and User2 only  
 User1, User2, and User4 only  
 User1, User2, User3, and User4

**NEW QUESTION 43**

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 46**

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- ? Contoso.com
- ? East.contoso.com

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest 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	Disabled

### USER SIGN-IN



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

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 authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="checkbox"/>	<input type="checkbox"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes  
 The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.  
 Box 2: No  
 The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.  
 Box 3: No  
 The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

**NEW QUESTION 48**

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

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

- A. Status only
- B. Status and Comment only
- C. Status and Severity only
- D. Status, Severity, and Comment only
- E. Status, Severity, Comment and Category

**Answer:** B

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations>

**NEW QUESTION 51**

- (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 54**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

You plan to create a new user named User1.

How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area. Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**NEW QUESTION 55**

HOTSPOT - (Topic 6)  
 HOTSPOT

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

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Add apps to the private store:

- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:

- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Add apps to the private store:

Install apps from the private store:

**NEW QUESTION 59**

- (Topic 6)

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

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

Answer: C

**NEW QUESTION 63**

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	Answer Area
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.	⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Actions**

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

**Answer Area**

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

**NEW QUESTION 65**

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 67**

- (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?

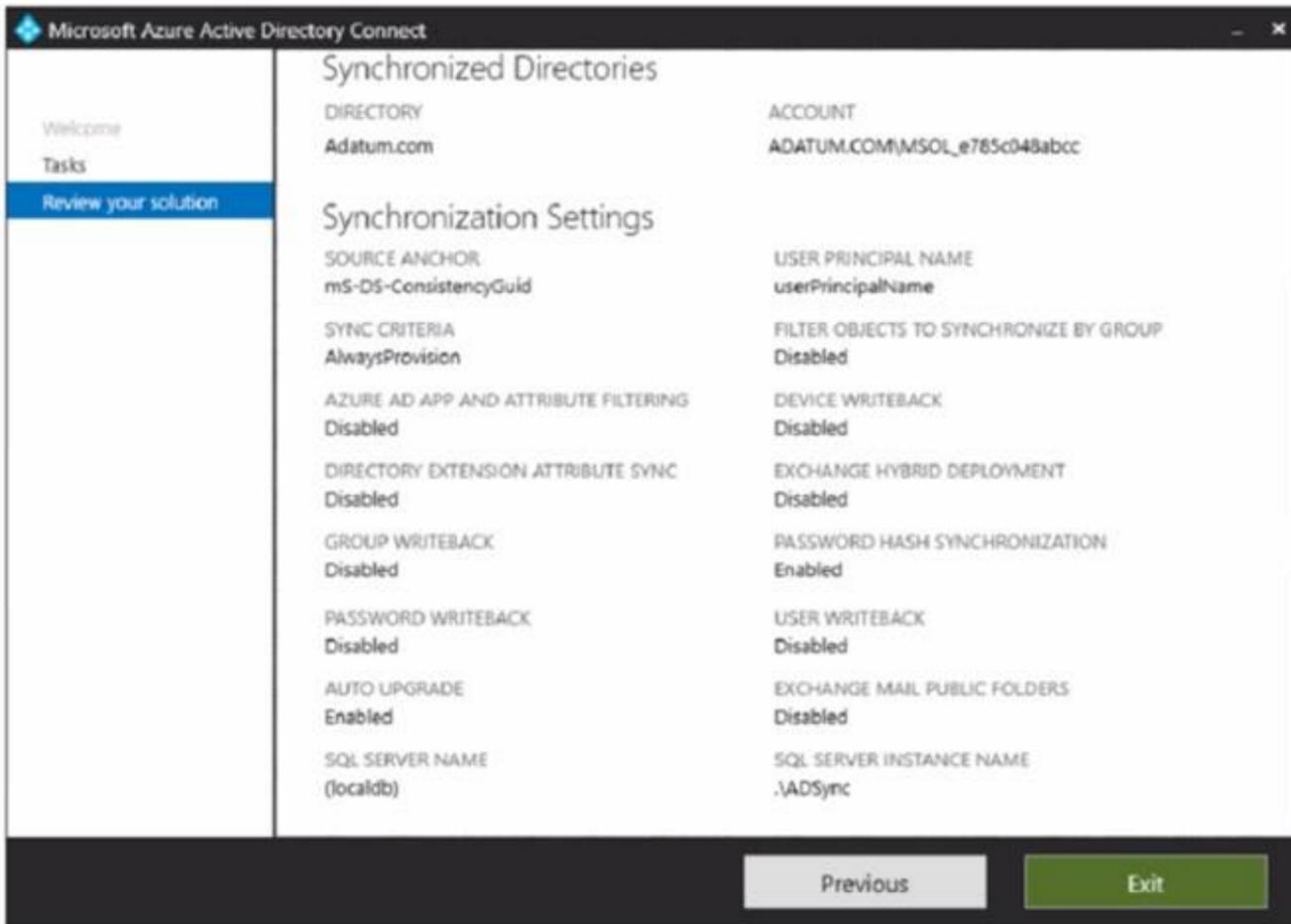
- A. information barriers
- B. communication compliance policies
- C. moderated distribution groups
- D. administrator units in Azure Active Directory (Azure AD)

**Answer:** A

**NEW QUESTION 72**

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.



An on-premises Active Directory user account named Allan You is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.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	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 76**

HOTSPOT - (Topic 6)

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

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

**NEW QUESTION 80**

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 81**

- (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 84**

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 87**

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the forest functional level to Windows Server 2016.

You copy the Group

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

Does this meet the goal?

- A. yes
- B. No

Answer: B

**NEW QUESTION 90**

- (Topic 6)

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

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

What should you use?

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

Answer: A

**NEW QUESTION 91**

HOTSPOT - (Topic 6)

**HOTSPOT**

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

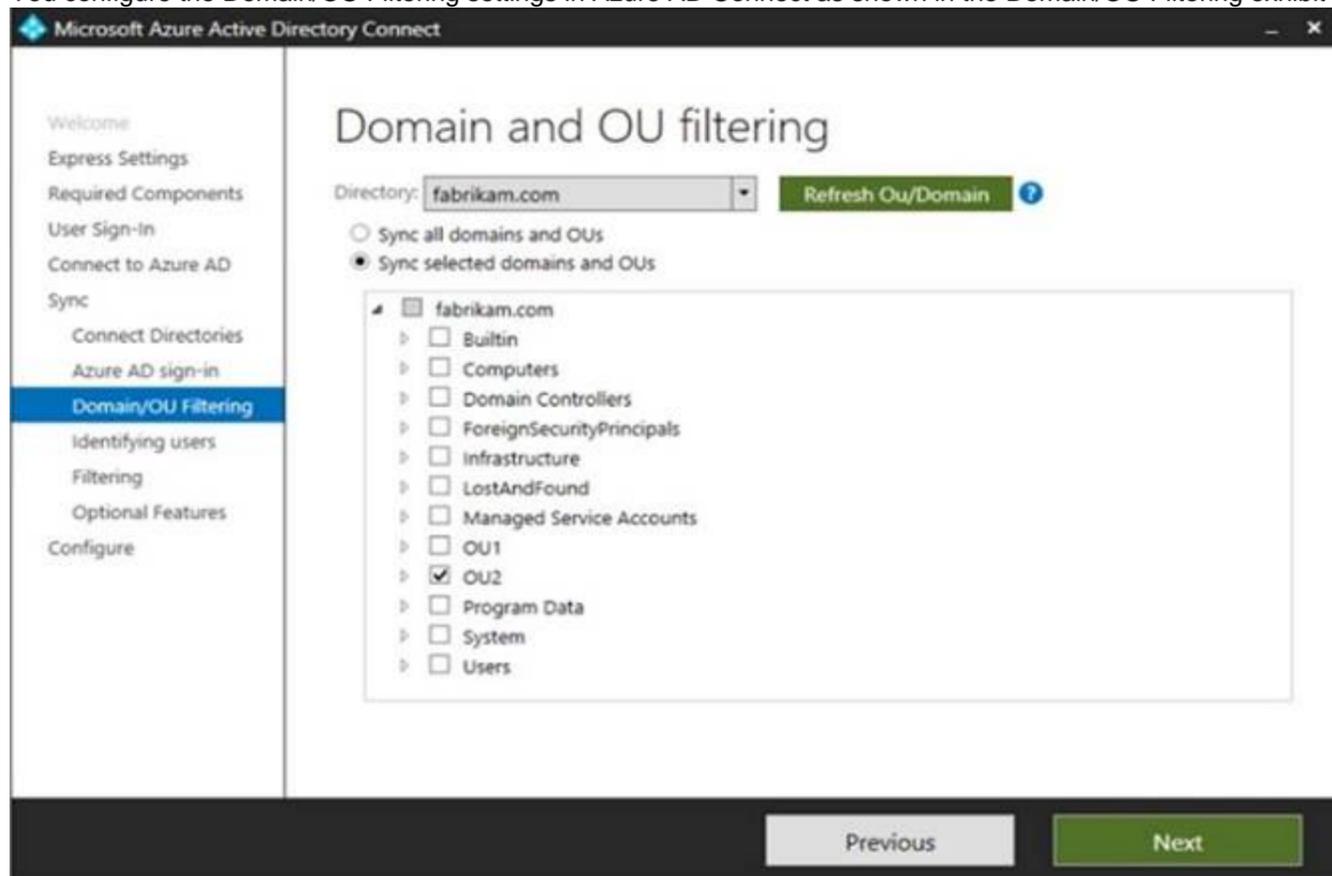
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

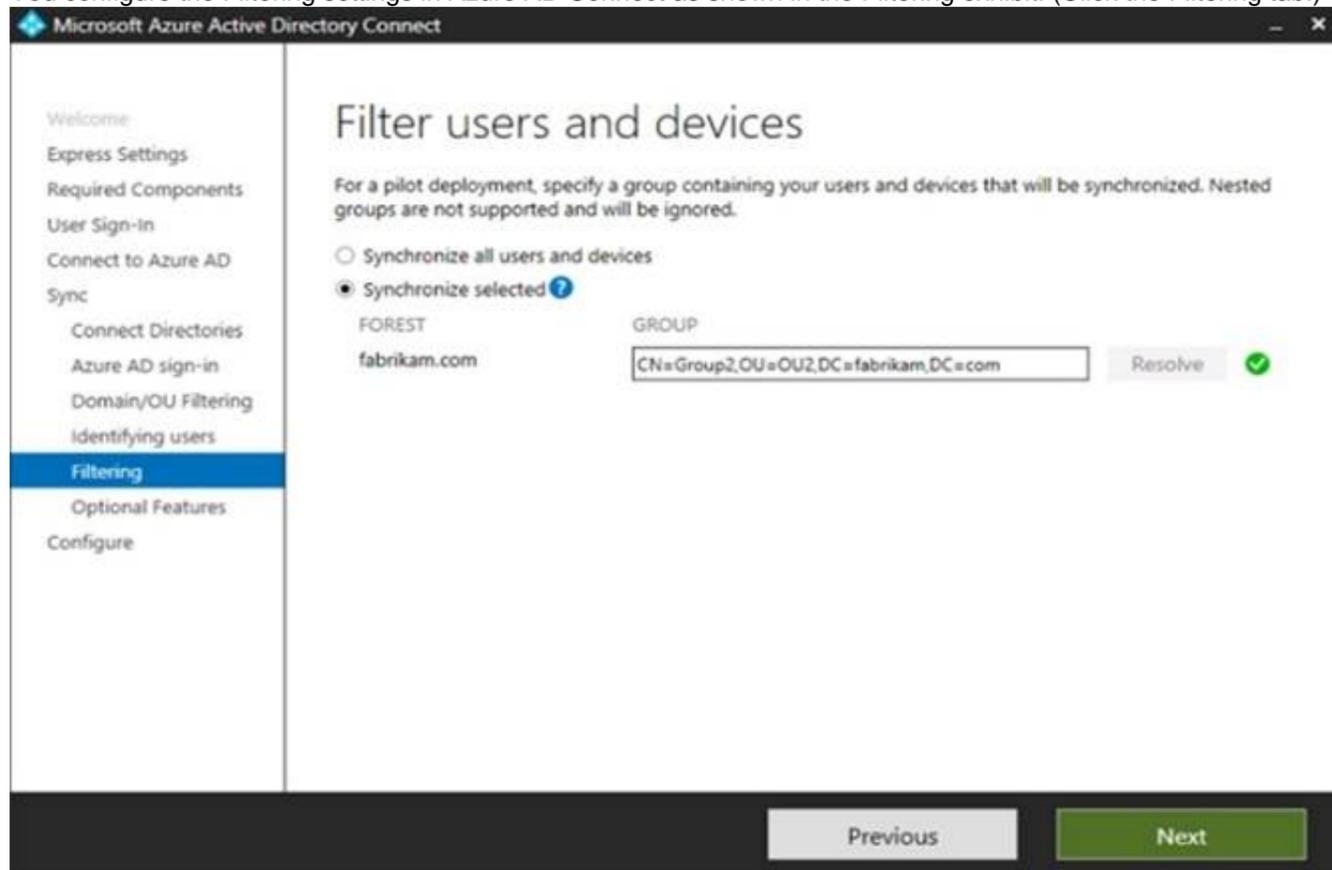
Group	Members
Group1	User1
Group2	User2, User3, Group1

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

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



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



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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

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

Box 2: Yes

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

Box 3: Yes

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

**NEW QUESTION 94**

- (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 97**

- (Topic 6)

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

**Answer:** B

**Explanation:**

Reference:

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

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

**NEW QUESTION 102**

- (Topic 6)

You have a Microsoft 365 tenant and a LinkedIn company page.

You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.

Where can you store data from the LinkedIn connector?

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

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 103**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to use a mailbox named Mailbox1 to analyze malicious email messages. You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- Ensure that incoming email is NOT filtered for Mailbox1.
- Detect impersonation and spoofing attacks on all other mailboxes in the subscription. Which two settings should you configure? To answer, select the appropriate settings in the answer area.

**Answer Area**

Policies	Rules
 Anti-phishing	 Tenant Allow/Block Lists
 Anti-spam	 Email authentication settings
 Anti-malware	 DKIM
 Safe Attachments	 Advanced delivery
 Safe Links	 Enhanced filtering
	 Quarantine policies

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

? Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

? Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

**NEW QUESTION 108**

- (Topic 6)

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy. What should you configure?

- A. actions
- B. incident reports
- C. exceptions
- D. user overrides

**Answer: D**

**Explanation:**

A DLP policy can be configured to allow users to override a policy tip and report a false positive.

You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word. If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.

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

**NEW QUESTION 113**

FILL IN THE BLANK - (Topic 6)

You have a Microsoft 365 subscription.

From 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 Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

A Yes

A. No

**Answer: A**

**NEW QUESTION 117**

- (Topic 6)

You have a Microsoft 365 tenant.

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

- A. Microsoft Cloud App Security
- B. Azure Sentinel
- C. Azure Web Application Firewall
- D. Azure Defender

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 121**

HOTSPOT - (Topic 6)

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

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

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

? Can be added to Compliance1 as recipients of noncompliance notifications

? Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Can be added to Compliance1 as recipients of noncompliance notifications:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

**NEW QUESTION 123**

DRAG DROP - (Topic 6)

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

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

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

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

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 127**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

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

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation

is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).

When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.

Box 2: Add trusted senders and domains Trusted senders and domains

Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

NEW QUESTION 128

- (Topic 6)

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 Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

- A. Yes
- B. no

Answer: B

NEW QUESTION 132

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 135

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

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

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

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

- 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.

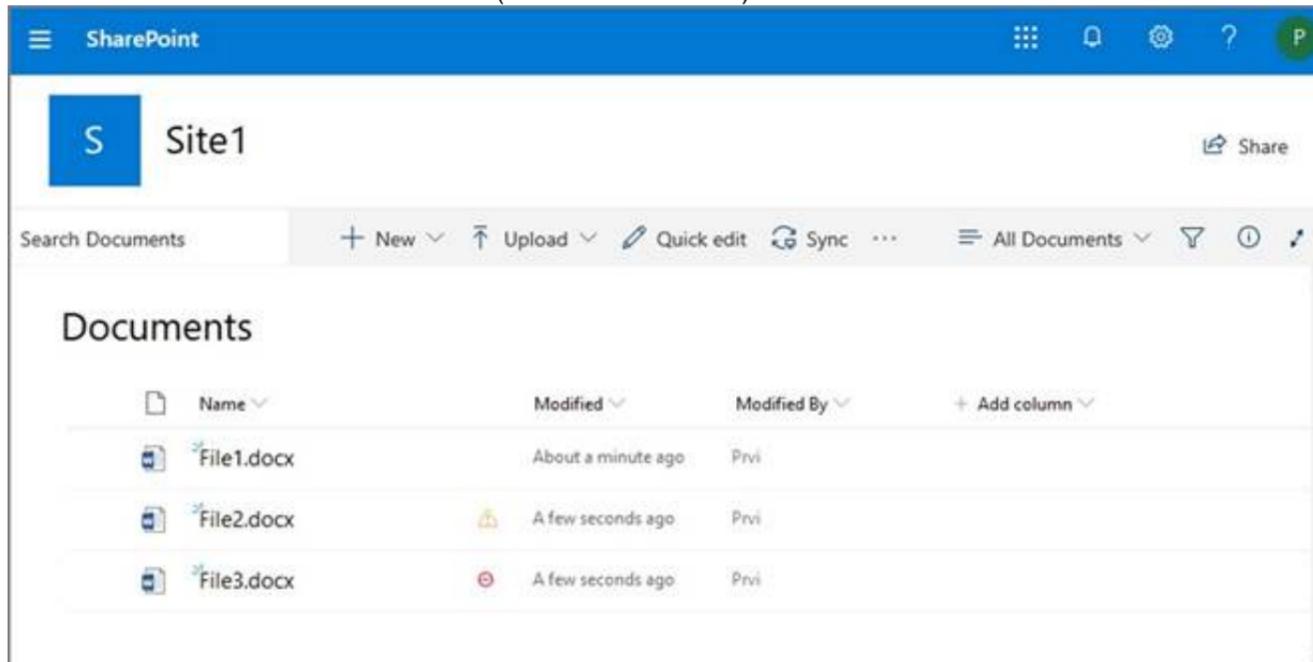
NEW QUESTION 136

HOTSPOT - (Topic 6)

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

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

**NEW QUESTION 138**

- (Topic 6)

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

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

Answer: C

Explanation:

Reference:

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

**NEW QUESTION 140**

- (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 142**

- (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 143**

- (Topic 6)

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

- Windows 10
- Android
- OS

On which devices can you configure the Endpoint DLP policies?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and macOS Only
- D. Windows 10, Android, and iOS

**Answer:** D

**Explanation:**

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

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

**NEW QUESTION 145**

HOTSPOT - (Topic 6)

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

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1: Microsoft Endpoint Manager  
 A local script  
 Group Policy  
 Microsoft Endpoint Manager  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

Device2: A local script  
 A local script  
 Group Policy  
 Microsoft Endpoint Manager  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1: Microsoft Endpoint Manager  
 A local script  
 Group Policy  
 Microsoft Endpoint Manager  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

Device2: A local script  
 A local script  
 Group Policy  
 Microsoft Endpoint Manager  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

NEW QUESTION 149

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: 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

**NEW QUESTION 154**

- (Topic 6)

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

Home > sensitivity

Labels Label policies Auto-labeling (preview)

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

+ Create a label Publish labels Refresh

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

Which labels can users apply to content?

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

**Answer: C**

**NEW QUESTION 157**

- (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 160**

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 163**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

- A. the Microsoft 365 admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft Defender for Cloud Apps portal
- D. the Microsoft Apps admin center

**Answer: C**

**NEW QUESTION 165**

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 168**

- (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 172**

- (Topic 6)

: 241

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

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

Answer: B

Explanation:

Reference:

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

**NEW QUESTION 174**

- (Topic 6)

Your company has a Microsoft E5 tenant.

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

What should you use?

- A. eDiscovery

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 178**

- (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 180**

- (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 assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

**NEW QUESTION 185**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint. You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

- A. a Microsoft Defender for Endpoint baseline profile
- B. an update policy for iOS
- C. a device configuration profile
- D. a mobile device management (MDM) security baseline profile

**Answer:** D

**NEW QUESTION 188**

- (Topic 6)

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements:

On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection
- C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- D. pass-through authentication

**Answer:** D

**Explanation:**

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same

passwords.

This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations

wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.

Password writeback is supported in environments that use the following hybrid identity models:

Password hash synchronization Pass-through authentication

Active Directory Federation Services

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

**NEW QUESTION 191**

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 True -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 193**

HOTSPOT - (Topic 6)

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

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Induce these users, groups and domains
  - o Users: User3
  - o Groups: Group1
- Exclude these users, groups and domains
  - o Groups: Group2
- Message limits

- o Set a daily message limit 100
- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains o Users: User1 o Groups: Group2
- Exclude these users, groups and domains o Users: User3
- Message limits
- o Set a daily message limit 50

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 send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 198**

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 203**

HOTSPOT - (Topic 6)

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

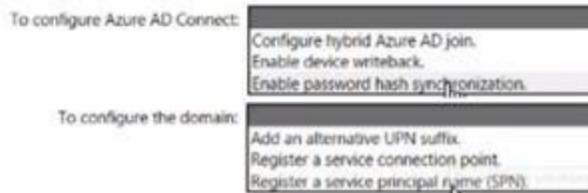
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

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

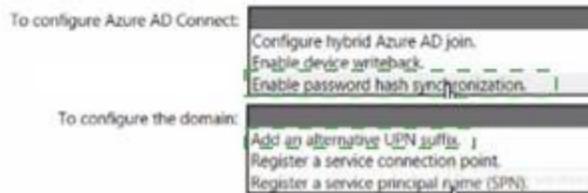


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 207**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.

You need to implement passwordless authentication. The solution must support all the devices.

Which authentication method should you use?

- A. Windows Hello
- B. FIDO2 compliant security keys
- C. Microsoft Authenticator app

Answer: C

**NEW QUESTION 209**

- (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 213**

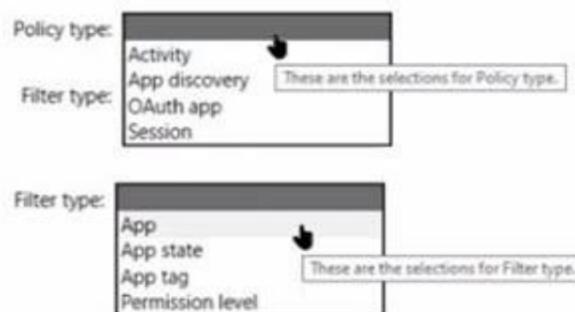
HOTSPOT - (Topic 6)

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

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

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

Answer Area

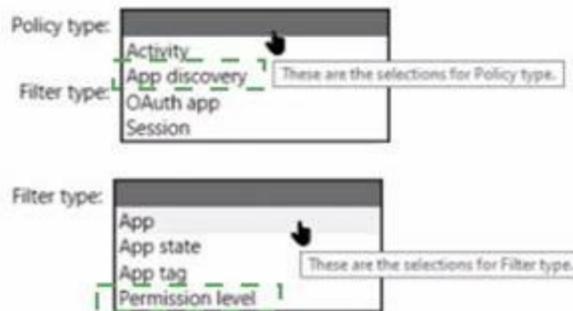


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 218**

- (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:

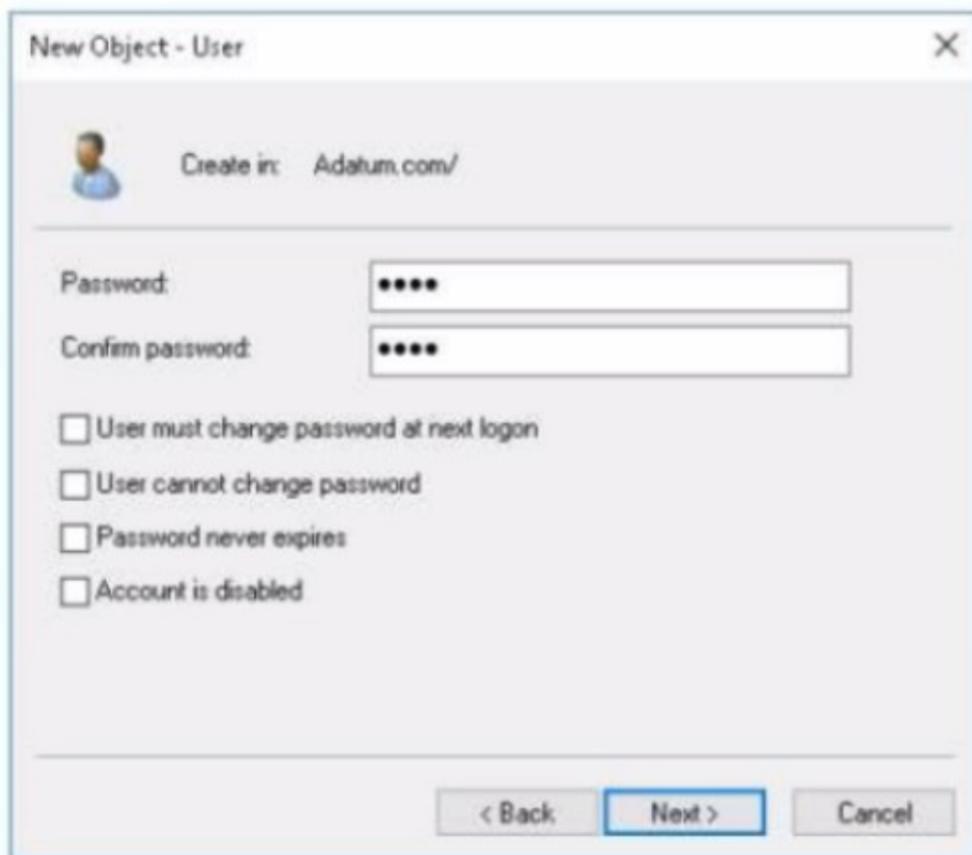
<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

**NEW QUESTION 222**

HOTSPOT - (Topic 6)

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

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



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

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

Days before a user is notified about 14 expiration

You confirm that User1 is synced to Azure AD.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

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

**NEW QUESTION 223**

HOTSPOT - (Topic 6)

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

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self- service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

User2:

User3:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

User1:   
 Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User2:   
 Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User3:   
 Security questions only  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

NEW QUESTION 227

HOTSPOT - (Topic 6)

You have device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 228

- (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 User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

**NEW QUESTION 233**

- (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 234**

- (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 237**

HOTSPOT - (Topic 6)

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

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

**Device limit restrictions**

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

Users may register their devices with Azure AD ⓘ

All None

**i** Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ

Yes No

Maximum number of devices per user ⓘ

5

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

**NEW QUESTION 242**

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 247**

- (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 248**

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 253**

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 255**

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**

<b>Retention period</b> 6 months <a href="#">Edit</a>	<b>Retention action</b> Retain and Delete <a href="#">Edit</a>
---	--

**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.)

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 260**

DRAG DROP - (Topic 6)  
 DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	File Server Resource Manager (FSRM)
Server2	Windows Server 2016	None

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.

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**

- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run GenConnectorConfig.ps1 on Server1.
- Run GenConnectorConfig.ps1 on Server2.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**

- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run GenConnectorConfig.ps1 on Server1.
- Run GenConnectorConfig.ps1 on Server2.

**Answer Area**

- Install the Microsoft Rights Management connector on Server2.
- Authorize Server1.
- Run GenConnectorConfig.ps1 on Server1.

**NEW QUESTION 262**

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- .xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

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

**Answer Area**

Office versions that require an add-in to support the sensitivity labels:

- Microsoft 365 Apps for enterprise and Office for the web only
- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only

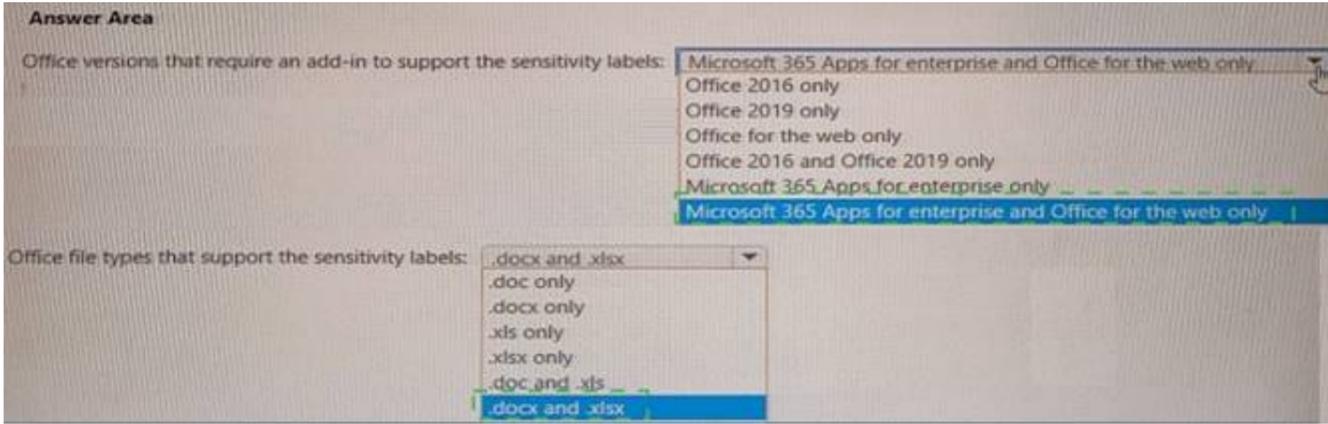
Office file types that support the sensitivity labels:

- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 265**

- (Topic 6)

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

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

**Answer: D**

**NEW QUESTION 266**

HOTSPOT - (Topic 6)

HOTSPOT

Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File type to use:

- CSV
- JSON
- PST
- XML

Required properties for each user:

- Display Name and Department
- First Name and Last Name
- User Name and Department
- User Name and Display Name

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

? Sign in to Microsoft 365 with your work or school account.

? In the admin center, choose Users > Active users.

? Select Add multiple users.

? On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.

? Etc.

Note: More information about how to add users to Microsoft 365 Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

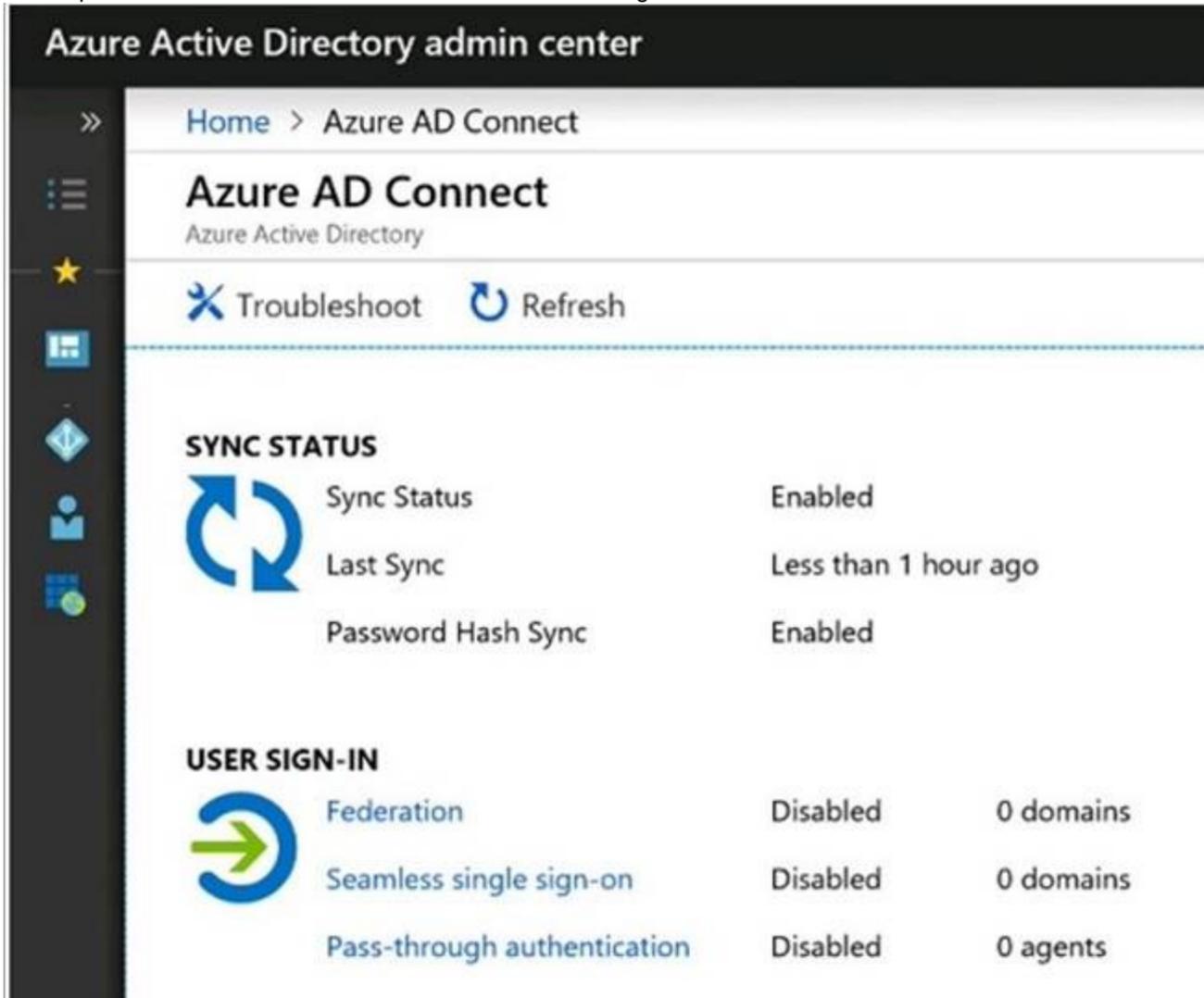
**NEW QUESTION 267**

HOTSPOT - (Topic 4)

HOTSPOT

You create the Microsoft 365 tenant.

You implement Azure AD Connect as shown in the following exhibit.



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**

During Project1, sales department users can access [answer choice] applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

- both on-premises and in the cloud
- in the cloud only
- on-premises only

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: only on-premises

In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.

In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.

Box 2: in the cloud only

**NEW QUESTION 272**

- (Topic 4)

You are evaluating the required processes for Project1.

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

Which DNS record should you recommend?

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

**Answer:** D

**Explanation:**

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

Note:

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

Text (TXT)

Mail exchanger (MX)

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

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

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

**NEW QUESTION 277**

- (Topic 4)

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

Which authentication strategy should you implement for the pilot projects?

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

**Answer:** C

**Explanation:**

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

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

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

Fabrikam does NOT plan to implement identity federation.

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

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

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

Reference:

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

**NEW QUESTION 280**

HOTSPOT - (Topic 3)

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Policy type:  

- Label
- Retention**
- Auto-labeling

Number of required policies:  

- 1
- 2**
- 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Policy type:  

- Label
- Retention
- Auto-labeling

Number of required policies:  

- 1
- 2
- 3

**NEW QUESTION 282**

- (Topic 3)

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

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

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 286**

- (Topic 3)

You need to create the DLP policy to meet the technical requirements. What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

**NEW QUESTION 289**

HOTSPOT - (Topic 3)

You plan to implement the endpoint protection device configuration profiles to support the planned changes.

You need to identify which devices will be supported, and how many profiles you should implement.

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

NOTE: Each correct selection is worth one point.

Supported devices:  

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

Number of required profiles:  

- 1
- 2
- 3
- 4
- 5

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Supported devices:

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

Number of required profiles:

1
2
3
4
5

**NEW QUESTION 294**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 295**

HOTSPOT - (Topic 2)

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker>

**NEW QUESTION 300**

HOTSPOT - (Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should

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

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

	▼
Audit log	
Data governance events	
DLP policy matches	
eDiscovery	

Filter by:

	▼
Activity	
Detail	
Item	
User agent	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results>

**NEW QUESTION 303**

- (Topic 2)

You need to recommend a solution for the security administrator. The solution must meet the technical requirements. What should you include in the recommendation?

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

**Answer:** B

**Explanation:**

References:

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

**NEW QUESTION 305**

- (Topic 1)

You need to create the Microsoft Store for Business. Which user can create the store?

- A. User2
- B. User3
- C. User4
- D. User5

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business>

**NEW QUESTION 307**

HOTSPOT - (Topic 1)

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

NOTE: Each correct selection is worth one point.

Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

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

References:

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

**NEW QUESTION 309**

HOTSPOT - (Topic 1)

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

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

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

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

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

References:

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

**NEW QUESTION 310**

- (Topic 1)

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

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

Answer: C

**Explanation:**

References:

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

**NEW QUESTION 313**

- (Topic 1)

You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

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

**Answer: C**

**NEW QUESTION 317**

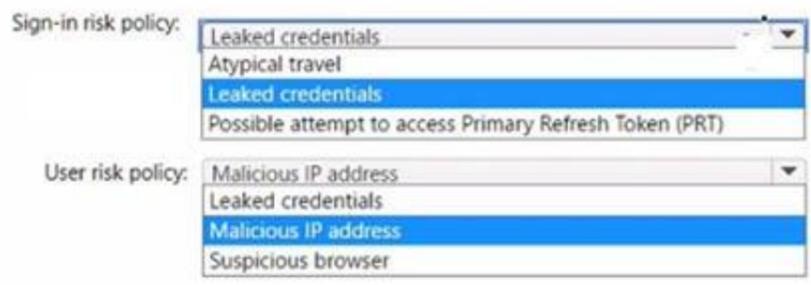
HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

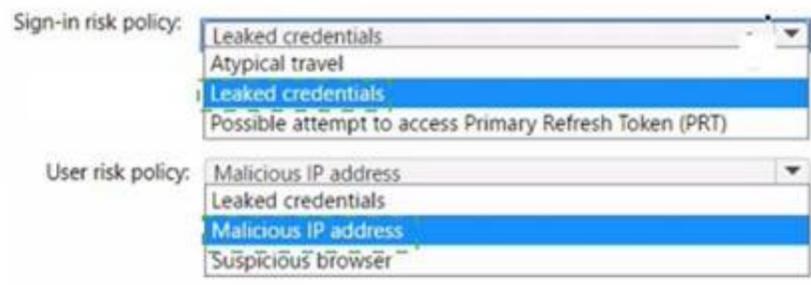


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area



**NEW QUESTION 319**

- (Topic 6)

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

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

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

What should you configure?

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

**Answer: D**

**NEW QUESTION 324**

- (Topic 6)

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

You need to be notified when a single user downloads more than 50 files during any 60- second period.

What should you configure?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an anomaly detection policy

**Answer: D**

**NEW QUESTION 327**

- (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 User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 328**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

More than or equal to  activities

During the last  minutes

On

- When the volume of matched activities becomes unusual

On

You need to identify the following:

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

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

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

NOTE: Each correct selection is worth one point.

How many days it will take to establish the baseline:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

How many days it will take to establish the baseline:

1
5
7
10

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

Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

**NEW QUESTION 332**

HOTSPOT - (Topic 6)

HOTSPOT

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

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

All the groups are deleted.

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

NOTE: Each correct selection is worth one point.

Groups that can be restored:

Group3 only
Group1 and Group2 only
Group2 and Group4 only
Group1, Group2, and Group3 only
Group1, Group2, Group3, and Group4

Retention period:

24 hours
7 days
14 days
30 days
90 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Group3 only

Box 2: 30 days

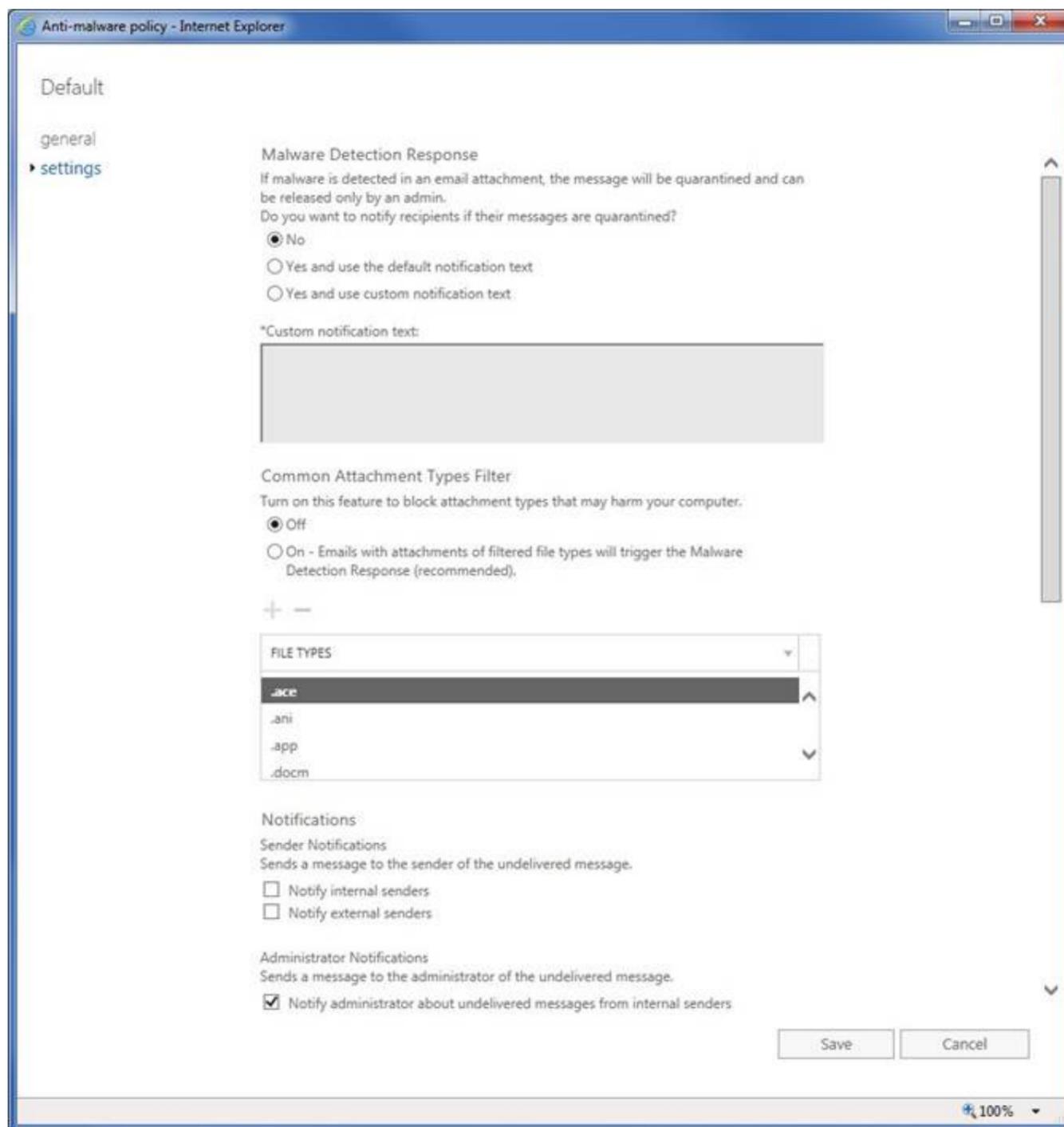
If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

**NEW QUESTION 337**

- (Topic 6)

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

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware. How will the email message and the attachments be processed?

- A. Both attachments will be remove
- B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
- C. The email message will be quarantined, and the message will remain undelivered.
- D. Both attachments will be remove
- E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed.'
- F. The malware-infected attachment will be remove
- G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies>

**NEW QUESTION 340**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must be blocked from signing in from outside the United States and Canada.

Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7
- F. 8

**Answer:** B

**Explanation:**

\* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

One Policy.

\* Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

One Policy.

\* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

One policy

\* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy

Reference:

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

**NEW QUESTION 344**

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

**Answer:** D

**Explanation:**

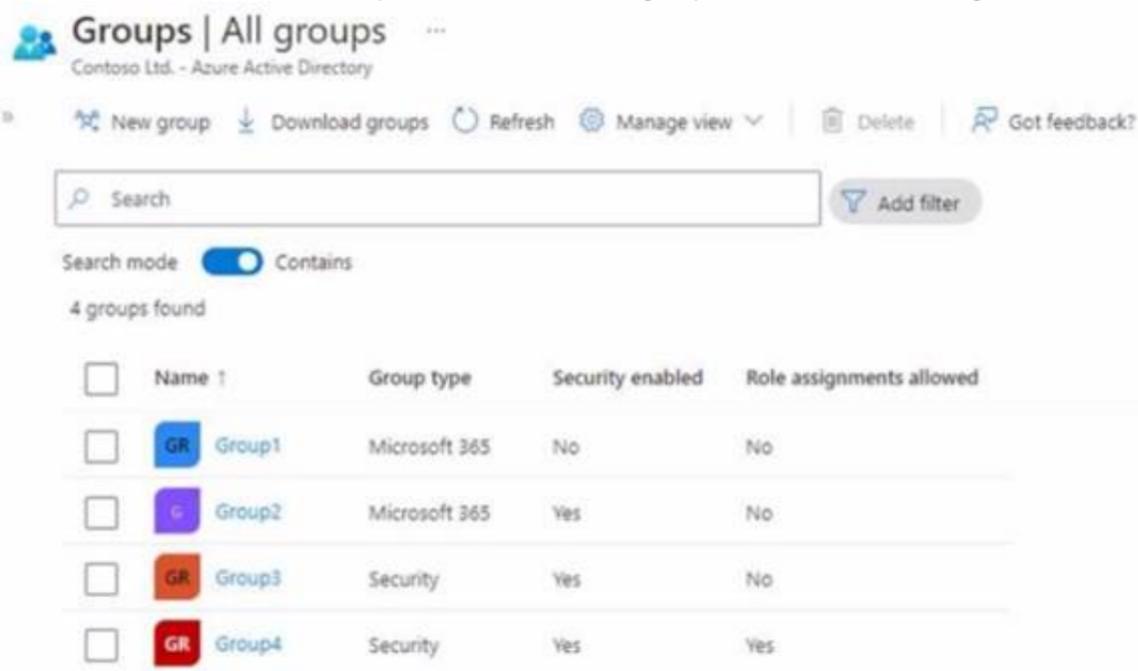
Reference:

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

**NEW QUESTION 348**

- (Topic 6)

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



To which groups can you assign Microsoft 365 E5 licenses?

- A. Group1 and Group2 only
- B. Group2 and Group3 only
- C. Group3 and Group4 only
- D. Group 1, Group2. and Group3 only
- E. Group2, Group3, and Group4 only

**Answer:** C

**NEW QUESTION 350**

- (Topic 6)

Your company has digitally signed applications.

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

What should you create in the Microsoft Defender Security Center?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 354**

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a computer that runs Windows 10.

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

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

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:  
<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

**NEW QUESTION 355**

- (Topic 6)

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

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

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

**Answer:** D

**Explanation:**

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

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

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

Reference:

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

**NEW QUESTION 356**

HOTSPOT - (Topic 6)

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Group1:  None of the groups  
 None of the groups  
 Group2 only  
 Group2 and Group4 only  
 Group2, Group4, Group5, and Group6 only  
 Group2, Group3, Group4, Group5, and Group6

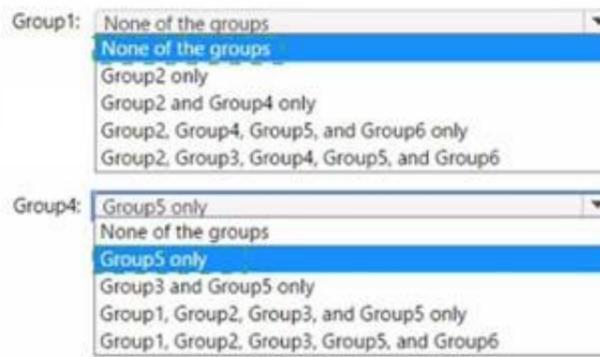
Group4:  Group5 only  
 None of the groups  
 Group5 only  
 Group3 and Group5 only  
 Group1, Group2, Group3, and Group5 only  
 Group1, Group2, Group3, Group5, and Group6

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Answer Area



**NEW QUESTION 360**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

- A. Create a Data Subject Request (DSR)
- B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
- C. Create an assessment based on the EU GDPR assessment template
- D. Create an assessment based on the Data Protection Baseline assessment template

Answer: C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

**NEW QUESTION 363**

- (Topic 6)

Your company has an Azure AD tenant named contoso.com that includes the users shown in the following table.

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	Not set	Group2
User3	Not set	Group1
User4	Canada	Group1

Group2 is a member of Group1.

You assign an Office 365 Enterprise E3 license to Group1. How many Office 365 E3 licenses are assigned?

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

Answer: C

**NEW QUESTION 364**

- (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 set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

**NEW QUESTION 365**

- (Topic 6)

Your company has a Microsoft 365 subscription. you implement sensitivity Doris for your company. You need to automatically protect email messages that contain the word Confidential in the subject line. What should you create?

- A. a sharing policy from the Exchange admin center
- B. a mail flow rule from the Exchange admin center
- C. a message Dace from the Microsoft 365 security center
- D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center

**Answer:** B

**NEW QUESTION 366**

- (Topic 6)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 370**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:

? Prevent users from enrolling personal devices.

? Ensure that users can enroll a maximum of 10 devices.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Prevent users from enrolling personal devices:

<input type="checkbox"/>	Conditional access policies
<input type="checkbox"/>	Device categories
<input type="checkbox"/>	Device limit restrictions
<input type="checkbox"/>	Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

<input type="checkbox"/>	Conditional access policies
<input type="checkbox"/>	Device categories
<input type="checkbox"/>	Device limit restrictions
<input type="checkbox"/>	Device type restrictions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Prevent users from enrolling personal devices:

<input type="checkbox"/>	Conditional access policies
<input type="checkbox"/>	Device categories
<input checked="" type="checkbox"/>	Device limit restrictions
<input checked="" type="checkbox"/>	Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

<input type="checkbox"/>	Conditional access policies
<input checked="" type="checkbox"/>	Device categories
<input checked="" type="checkbox"/>	Device limit restrictions
<input type="checkbox"/>	Device type restrictions

**NEW QUESTION 372**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.

You create an Android app protection policy named Policy1 that is targeted to all Microsoft apps and assigned to all users.

Policy1 has the Data protection settings shown in the following exhibit.

Data Transfer

Backup org data to Android backup services  Allow  Block

Send org data to other apps  Policy managed apps

Select apps to exempt

Save copies of org data  Allow  Block

Allow user to save copies to selected services  SharePoint

Transfer telecommunication data to  Any dialer app

Dialer App Package ID

Dialer App Name

Receive data from other apps  All Apps

Open data into Org documents  Allow  Block

Allow users to open data from selected services  3 selected

Restrict cut, copy, and paste between other apps  Policy managed apps with paste in

Screen capture and Google Assistant  Allow  Block

Approved keyboards  Require  Not required

Select keyboards to approve

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

A user can copy files from Microsoft OneDrive to [answer choice] only.

Microsoft SharePoint Online  
 OneDrive  
 local storage  
 Microsoft SharePoint Online  
 Microsoft SharePoint Online and OneDrive

A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

any app  
 any app  
 only managed apps  
 only unmanaged apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

A user can copy files from Microsoft OneDrive to [answer choice] only.

Microsoft SharePoint Online  
 OneDrive  
 local storage  
 Microsoft SharePoint Online  
 Microsoft SharePoint Online and OneDrive

A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

any app  
 any app  
 only managed apps  
 only unmanaged apps

**NEW QUESTION 376**

HOTSPOT - (Topic 6)

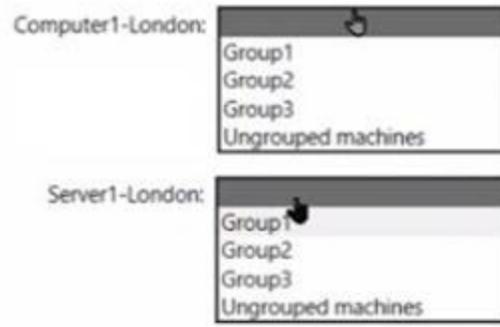
You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	Not applicable

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

Answer Area

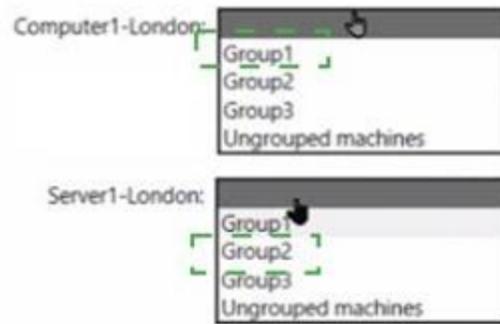


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 381**

HOTSPOT - (Topic 6)

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

From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? 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 383**

.....

## 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