



# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

References:

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

#### NEW QUESTION 2

- (Exam Topic 1)

On which server should you install the Azure ATP sensor?

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

**Answer:** A

#### Explanation:

References:

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

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

#### NEW QUESTION 3

- (Exam Topic 1)

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

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure a pilot for co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client>

#### NEW QUESTION 4

- (Exam Topic 2)

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

**Answer:** A

#### NEW QUESTION 5

- (Exam Topic 2)

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

What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection

- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

**Answer:** B

**Explanation:**

References:

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

**NEW QUESTION 6**

- (Exam Topic 3)

You create the planned DLP policies.

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 7**

- (Exam Topic 3)

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 8**

- (Exam Topic 5)

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

- A. Enable auditing.
- B. Enable Microsoft 365 usage analytics.
- C. Create an Insider risk management policy.
- D. Create a communication compliance policy.

**Answer:** A

**Explanation:**

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview> <https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

**NEW QUESTION 9**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

12 items

Search

Filter

Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

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

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

Answer: ABC

Explanation:

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

NEW QUESTION 10

- (Exam Topic 5)

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

Actions

Answer Area

Deploy Azure Active Directory (Azure AD) Application Proxy.

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

Sign in to App1.

Create a conditional access policy.

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

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

⬅️

➡️

⬆️

⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security>

NEW QUESTION 10

- (Exam Topic 5)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

##### Azure AD Connect sync

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

#### USER SIGN-IN



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

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.  
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.  
Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

This is not a permissions issue.

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

#### NEW QUESTION 15

- (Exam Topic 5)

Your company has a Microsoft 365 tenant

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

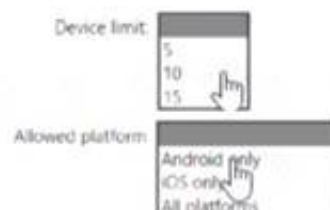
The device type restriction are configured as shown in the following table.

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

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

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

Answer Area



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restricti>

#### NEW QUESTION 20



- (Exam Topic 5)

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

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

You need to prevent devices that do not meet the requirements from accessing resources in the tenant. Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

**Answer: BD**

**Explanation:**

Reference:

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

**NEW QUESTION 22**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Social engineering technique:

▼

Credential harvest  
Link to malware  
Malware attachment

Training experience:

▼

Identity Theft  
Mass Market Phishing  
Web Phishing

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Credential Harvest

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

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

Malware Attachment Link to Malware Etc.

Box 2: Mass Market Phishing Reference:

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

**NEW QUESTION 27**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

- A. From the Microsoft Entra admin center, create a conditional access policy
- B. From the Microsoft 365 admin center, configure the Modern authentication settings.
- C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
- D. From Multi-Factor Authentication, configure the service settings.

**Answer: A**

**Explanation:**

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati>

#### NEW QUESTION 32

- (Exam Topic 5)

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 37

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

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

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

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

**Answer: C**

#### Explanation:

Reference:

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

#### NEW QUESTION 42

- (Exam Topic 5)

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 47

- (Exam Topic 5)

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

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

NOTE: Each correct selection is worth one point.

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

**Answer: ABE**

#### Explanation:

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

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

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

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

(A) In your on-premises environment

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

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



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

\* 4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

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

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

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

#### NEW QUESTION 49

- (Exam Topic 5)

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

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

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

NOTE: Each correct selection is worth one point.

In Azure:

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

On the computers:

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

A. Mastered

B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer>

#### NEW QUESTION 50

- (Exam Topic 5)

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

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

You have a computer that runs Windows 10.

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

Solution: From the Settings app, you select Update & Security to view the update history.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### NEW QUESTION 55

- (Exam Topic 5)

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

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

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

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

A. Device2 only

B. Device1 and Device3 only

C. Device2 and Device4 only

D. Device2, Device3, and Device5 only

E. Device1, Device2, Device3, Device4, and Device5

Answer: C

NEW QUESTION 58

- (Exam Topic 5)

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>

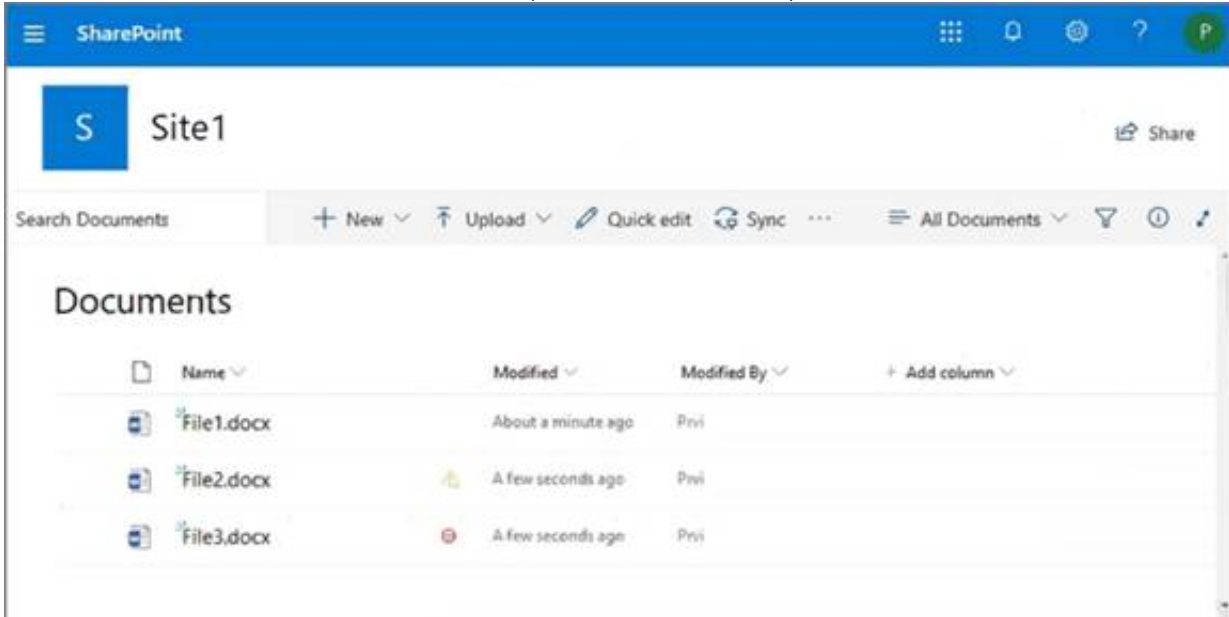
NEW QUESTION 61

- (Exam Topic 5)

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:

Graphical user interface, text, application, email Description automatically generated  
Reference:  
<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/> <https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/>

### NEW QUESTION 63

- (Exam Topic 5)

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 64

- (Exam Topic 5)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Devices that can onboard to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Text, table Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?vie>

### NEW QUESTION 67

- (Exam Topic 5)

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.

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

Answer Area

Computer1-London:

▼

Group1

Group2

Group3

Ungrouped machines

Server1-London:

▼

Group1

Group2

Group3

Ungrouped machines

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1-London:

▼

Group1

Group2

Group3

Ungrouped machines

Server1-London:

▼

Group1

Group2

Group3

Ungrouped machines

NEW QUESTION 71

- (Exam Topic 5)

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 75

- (Exam Topic 5)

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

- A. From the Exchange admin center create a mail flow rule.
- B. From Microsoft 365 Defender, start a message trace.
- C. From Microsoft Defender for Cloud Apps, create an activity policy.
- D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer: D

NEW QUESTION 80

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

- > Captures Microsoft Teams channel messages that contain threatening or violent language.



➤ Alerts a reviewer when a threatening or violent message is identified.  
What should you include in the solution?

- A. Data Subject Requests (DSRs)
- B. Insider risk management policies
- C. Communication compliance policies
- D. Audit log retention policies

**Answer:** C

#### NEW QUESTION 82

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has the files in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	5

The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data loss prevention (DLP) policy named Policy1 as shown in the following exhibit.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Review your settings

Template name  
Custom policy  
Edit

Policy name  
Policy1  
Edit

Description  
Edit

Applies to content in these locations  
SharePoint sites  
Edit

Policy settings  
If the content contains these types of sensitive info: IP Address  
then notify people with a policy tip and email message.  
  
If there are at least 2 instances of the same type of sensitive info,  
block access to the content.  
  
Turn policy on after it's created?  
Yes  
Edit

How many files will be visible to user1 and User2 after Policy1 is applied to answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

#### Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5



- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

### Answer Area

User1:

User2:

### NEW QUESTION 87

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

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

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

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

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

**Answer:** D

**Explanation:**

Self-remediation with self-service password reset

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

Reference:

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

### NEW QUESTION 90

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

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

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

### Answer Area

Teams daily active users:

Recent Microsoft service issues:

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

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

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

Box 2: Service Health

Recent Microsoft service issues

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

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-usage-activity> <https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

#### NEW QUESTION 91

- (Exam Topic 5)

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



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

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

**Answer: B**

#### NEW QUESTION 94

- (Exam Topic 5)

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:

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.

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 99**

- (Exam Topic 5)

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
<b>Threat protection status</b>
URL threat protection

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

Mailflow status report
<b>Mailflow status report</b>
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
<b>Threat protection status</b>
URL threat protection

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

Mailflow status report
<b>Mailflow status report</b>
Spoof detections
Threat protection status
URL threat protection

**NEW QUESTION 101**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

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

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

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

**Answer:** C

**Explanation:**

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

Reference:

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

**NEW QUESTION 102**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

- A. Policy1 and Policy2 only
- B. Policy2 and Policy4 only
- C. Policy3 and Policy4 only
- D. Policy1 and Policy3only

**Answer:** A

**NEW QUESTION 106**

- (Exam Topic 5)

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 110**

- (Exam Topic 5)

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 115

- (Exam Topic 5)

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 119

- (Exam Topic 5)

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

##### Azure AD Connect sync

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

#### USER SIGN-IN



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

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

Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 120

- (Exam Topic 5)

HOTSPOT

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



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

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

Assignments:

- Users and groups: Group1
- Cloud apps or actions: All cloud apps
- > Access controls:
- > Grant, require multi-factor authentication
- > Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

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

- > Conditional Access policies can be enabled in report-only mode.
- > During sign-in, policies in report-only mode are evaluated but not enforced.
- > Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- > Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-on>

#### NEW QUESTION 121

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

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

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

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

**Answer: B**

#### NEW QUESTION 124

- (Exam Topic 5)

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:

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

NEW QUESTION 129

- (Exam Topic 5)  
HOTSPOT

You have a Microsoft 365 E5 subscription.  
From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

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

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

User	Date
User1	August 5
User2	August 7

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

User1: 

▼

August 6

August 17

August 19

September 3

September 5

User2: 

▼

August 8

August 17

August 19

August 21

September 7

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Box 1: August 19

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

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

Box 2: August 21 Reference:

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

NEW QUESTION 131

- (Exam Topic 5)

HOTSPOT

			progress	actions	status			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

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

Answer Area

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 136

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:  
Manage Microsoft Exchange Online settings.

Create Microsoft 365 groups.  
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.  
What should you use?

- A. Azure AD Identity Protection
- B. Microsoft Entra Verified ID
- C. Conditional Access
- D. Azure AD Privileged Identity Management (PIM)

**Answer:** D

**Explanation:**

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:  
Provide just-in-time privileged access to Azure AD and Azure resources  
Assign time-bound access to resources using start and end dates  
Require approval to activate privileged roles  
Enforce multi-factor authentication to activate any role  
Use justification to understand why users activate  
Get notifications when privileged roles are activated  
Conduct access reviews to ensure users still need roles  
Download audit history for internal or external audit  
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

**NEW QUESTION 139**

- (Exam Topic 5)

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

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

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

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

**Answer:** D

**Explanation:**

Disabled accounts  
Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.  
The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.  
Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and>

**NEW QUESTION 143**

- (Exam Topic 5)

HOTSPOT

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

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

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



Answer Area

Microsoft 365 setting:

Office installation options

Privileged access

Release preferences

User:

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:

Office installation options

Privileged access

Release preferences

User:

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

NEW QUESTION 146

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.

For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Activities to search for:

Exchange mailbox activities

Site administration activities

Show results for all activities

Role administration activities

Field to filter by:

Item

User

Detail

IP address

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Activities to search for:

▼

Exchange mailbox activities  
Site administration activities  
Show results for all activities  
Role administration activities

Field to filter by:

▼

Item  
User  
Detail  
IP address

#### NEW QUESTION 149

- (Exam Topic 5)

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

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

**Answer: C**

#### NEW QUESTION 150

- (Exam Topic 5)

You have an Azure AD tenant.

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

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

What should you do?

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

**Answer: B**

#### NEW QUESTION 155

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

**Answer: C**

#### NEW QUESTION 157

- (Exam Topic 5)

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 160**

- (Exam Topic 5)

**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:	<div><div></div><div>An allow or block file</div><div>A file indicator</div><div>A remediation request</div><div>An update ring</div></div>
Block an application executable based on a file hash:	<div><div></div><div>An allow or block file</div><div>A file indicator</div><div>A remediation request</div><div>An update ring</div></div>

- 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.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln-ap>

**NEW QUESTION 165**

- (Exam Topic 5)

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.

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform. Which two tasks should you identify? Each correct answer presents a complete solution.  
NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

**Answer:** AE

**Explanation:**

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below). Only on users who are non-admins or in any of the following limited admin roles:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator Reference:

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

**NEW QUESTION 169**

- (Exam Topic 5)

Your company has multiple offices.

You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator. You need to ensure that the local administrators can manage only the devices in their respective office. What should you use?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 173**

- (Exam Topic 5)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription. You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 174**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

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

- Opening files in Microsoft SharePoint that contain malicious content
- Impersonation and spoofing attacks in email messages

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

NOTE: Each correct selection is worth one point.

Answer Area

Opening files in SharePoint that contain malicious content:

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:  
Answer Area

Opening files in SharePoint that contain malicious content:

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

Anti-spam

Anti-Phishing

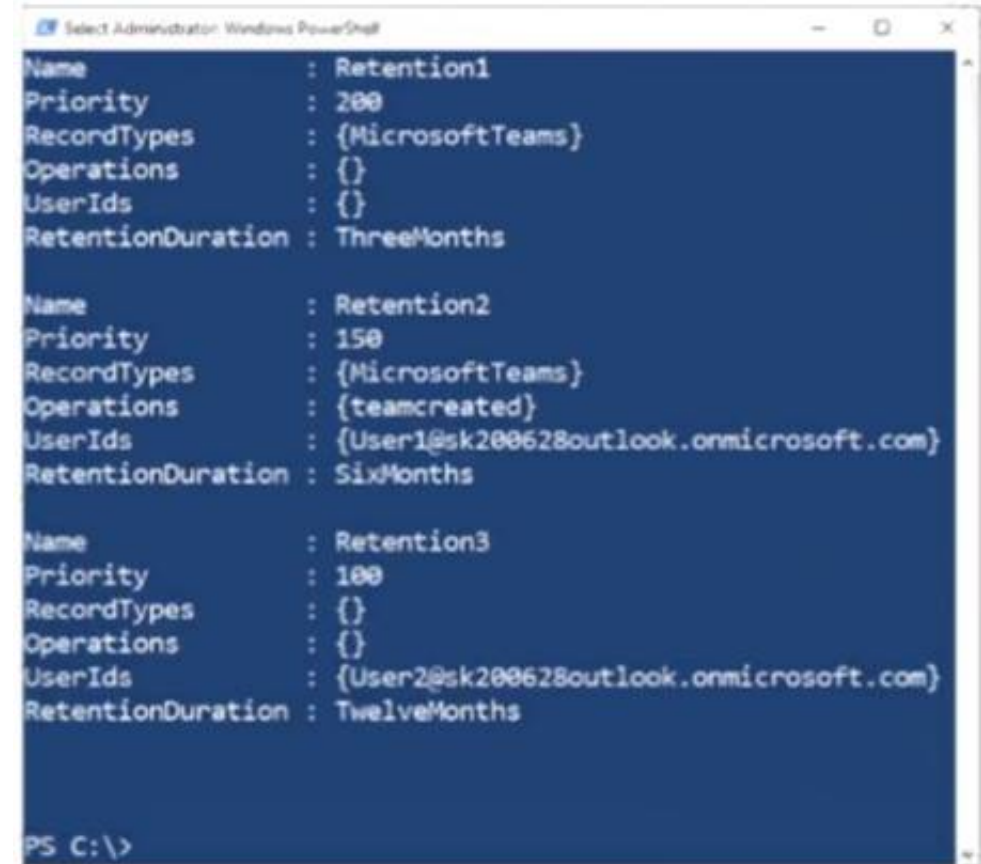
Safe Attachments

Safe Links

NEW QUESTION 179

- (Exam Topic 5)

You have a Microsoft 365 ES subscription that has three auto retention policies as show 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

If User1 creates a team in Microsoft Teams, the event is [answer choice]

not retained

retained for 90 days

retained for six months

retained for one year

If User2 adds a channel in Microsoft Teams, the event is [answer choice]

not retained

retained for 90 days

retained for six months

retained for one year

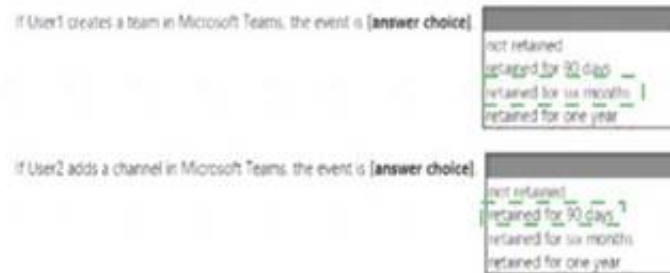
- A. Mastered  
B. Not Mastered



Answer: A

**Explanation:**

Answer Area



**NEW QUESTION 183**

- (Exam Topic 5)

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

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

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

- > To all users, deploy an Office 365 E3 license without the Power Automate license option.
- > To all users, deploy an Enterprise Mobility + Security E5 license.
- > To the users in the research department only, deploy a Power BI Pro license.
- > To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

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

Answer: C

**Explanation:**

One for all users, one for the research department, and one for the marketing department. Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers

on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

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

**NEW QUESTION 188**

- (Exam Topic 5)

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 189**

- (Exam Topic 5)

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 checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 191

- (Exam Topic 5)  
HOTSPOT

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

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.  
How should you complete the membership rule? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

(user.userType 

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department 

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory Supported expression operators  
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

- \* Equals
- eq
- \* Contains
- contains
- \* Etc.

Box 2: -contains "Support" Incorrect:  
\* -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.  
Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

NEW QUESTION 196

- (Exam Topic 5)  
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:**

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manage>

**NEW QUESTION 198**

- (Exam Topic 5)

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

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

You plan to publish a sensitivity label named Label1. To which groups can you publish Label1?

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

**Answer:** A

**Explanation:**

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

Reference:

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

**NEW QUESTION 203**

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps. You configure a session control policy to block downloads from SharePoint Online sites. Users report that they can still download files from SharePoint Online sites.

You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites. What should you configure?

- A. an access policy
- B. a data loss prevention (DLP) policy
- C. an activity policy
- D. a Conditional Access policy

**Answer:** A

**NEW QUESTION 206**

- (Exam Topic 5)

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

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

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

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

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.  
You need to configure the Windows Update for Business Group Policy settings on Server1.  
Solution: You raise the domain functional level to Windows Server 2019. 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 211

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

- A. Perform a content search
- B. Create a supervision policy
- C. Create an eDiscovery case
- D. Perform an audit log search

**Answer: D**

#### NEW QUESTION 213

- (Exam Topic 5)

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 217

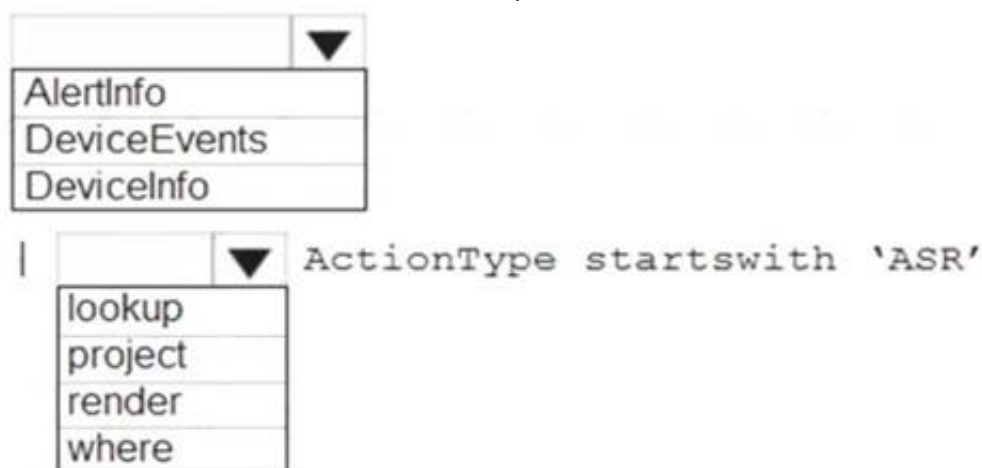
- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace. You need to find the ASR rules that match the activities on the devices.

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Graphical user interface, application Description automatically generated

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction>

#### NEW QUESTION 218

- (Exam Topic 5)

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

Company policy requires that the devices have the following configurations:

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

You need to configure the devices to meet the requirements. What should you use?

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 220**

- (Exam Topic 5)

**HOTSPOT**

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

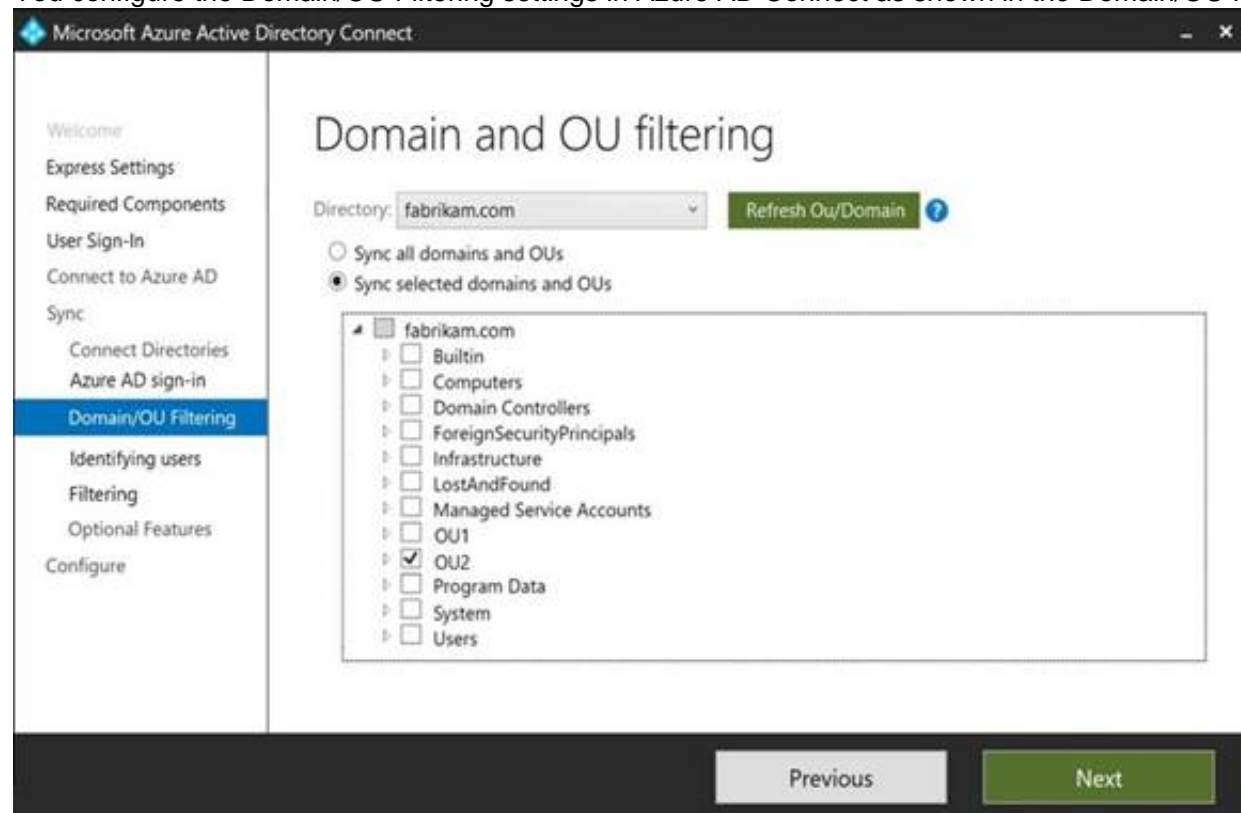
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group – Global	OU1
User3	User	OU2
Group2	Security Group – Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

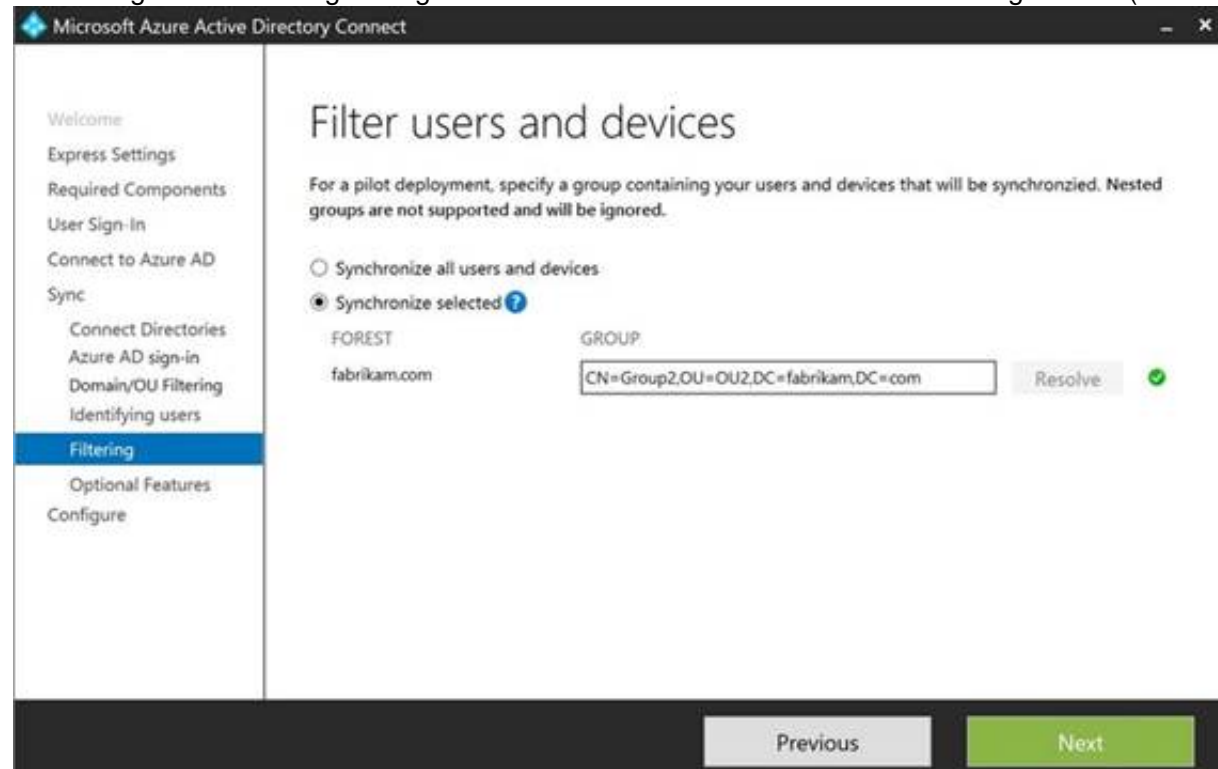
You are configuring synchronization between fabrikam.com and an Azure AD tenant.

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.)



The screenshot shows the 'Domain and OU filtering' configuration window in Microsoft Azure Active Directory Connect. The 'Directory' is set to 'fabrikam.com'. The 'Sync selected domains and OUs' option is selected. The list of OUs includes 'fabrikam.com', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Infrastructure', 'LostAndFound', 'Managed Service Accounts', 'OU1', 'OU2' (which is checked), 'Program Data', 'System', and 'Users'. The 'Previous' and 'Next' buttons are visible at the bottom.

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



The screenshot shows the 'Filter users and devices' configuration window in Microsoft Azure Active Directory Connect. The 'Synchronize selected' option is selected. The 'FOREST' is set to 'fabrikam.com'. The 'GROUP' is set to 'CN=Group2,OU=OU2,DC=fabrikam,DC=com'. The 'Resolve' button is visible next to the group name. The 'Previous' and 'Next' buttons are visible at the bottom.

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. Reference:

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

### NEW QUESTION 221

- (Exam Topic 5)

You have a Microsoft 365 subscription.

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

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

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

- A. Yes  
B. No

**Answer:** B

### NEW QUESTION 224

- (Exam Topic 5)

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

New audit retention policy
✕

**Name \***

**Description**

**Record Types**

**Activities**

**Users:**

**Duration \***

☐ 90 Days  
☒ 6 Months  
☐ 1 Year

**Priority \***

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.

Admin1:

▼

30 days  
 90 days  
 6 months  
 1 year

Admin2:

▼

30 days  
 90 days  
 6 months  
 1 year

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Admin1:

▼

30 days  
 90 days  

6 months

  
 1 year

Admin2:

▼

30 days  

90 days

  
 6 months  
 1 year

#### NEW QUESTION 228

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains a user named User1. You plan to implement insider risk management. You need to ensure that User1 can perform the following tasks:

- > Review alerts.
- > Manage cases.
- > Create notice templates.
- > Review user emails by using Content explorer. The solution must use the principle of least privilege. To which role group should you add User1?

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 233**

- (Exam Topic 5)

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

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

Azure AD Connect has the following settings:

- > Password Hash Sync: Enabled
- > Pass-through authentication: Enabled

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 238**

- (Exam Topic 5)

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

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

You have a computer that runs Windows 10.

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

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 240**

- (Exam Topic 5)

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

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

You have a computer that runs Windows 10.

You need to verify which version of Windows 10 is installed. Solution: At a command prompt, you run the winver.exe command. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:

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

#### NEW QUESTION 244

- (Exam Topic 5)

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

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

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 249

- (Exam Topic 5)

HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

- > Scope type: Directory
- > Selected members: Group1
- > Assignment type: Active
- > Assignment starts: Mar 15, 2023
- > Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

- > Scope type: Directory
- > Selected members: Group2
- > Assignment type: Eligible
- > Assignment starts: Jun 15, 2023
- > Assignment ends: Oct 15, 2023

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

NOTE: Each correct selection is worth one point.

#### Answer Area

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Yes

Admin1 is member of Group1.

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

July 15, 2023 is with the assignment period.

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

Box 2: No

Admin2 is member of Group2.

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

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

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

Box 3: Yes

Admin3 is member of Group1 and Group2.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

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

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



NEW QUESTION 250

- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.  
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
You have a Microsoft 365 E5 subscription 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/pe>

NEW QUESTION 253

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription. Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.  
NOTE: Each correct selection is worth one point.

- A. Anti-malware
- B. Anti-phishing
- C. Safe Attachments
- D. Anti-spam
- E. Safe Links

Answer: CE

NEW QUESTION 257


- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.  
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
Your network contains an on-premises Active Directory domain 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 259

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

**Name**  
Sensitivity1

**Display name**  
Sensitivity1

**Description for users**  
Sensitivity1

**Scope**  
File.Email

**Encryption**

**Content marking**  
Watermark: Watermark  
Header: Header

**Auto-labeling**

**Group settings**

**Site settings**

**Auto-labeling for database columns**  
None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

Edit Policy

Delete Policy

**Policy name**  
Auto-labeling policy

**Description**

**Label in simulation**  
Sensitivity1

**Info to label**  
IP Address

**Apply to content in these locations**  
Exchange email All

**Rules for auto-applying this label**  
Exchange email 1 rule

**Mode**  
On

**Comment**

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 263**

- (Exam Topic 5)

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery
- E. attack surface reduction (ASR)

**Answer:** BE

**Explanation:**

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting

The Microsoft 365 Defender portal (<https://security.microsoft.com>) provides easy access to information about detected threats and actions to address those threats.

The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created.

The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.

The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.

The Reports section includes reports that show threats detected and their status. E: What can you expect from Microsoft Defender for Endpoint P1?

Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:

Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.

(E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.

Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.

The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

\*\*Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1> <https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan>

**NEW QUESTION 264**

- (Exam Topic 5)

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

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

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

**Answer:** C

**NEW QUESTION 265**

- (Exam Topic 5)

HOTSPOT

You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.

A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

MFA method:

Call to phone

Email message

Security questions

Text message to phone

Notification to Microsoft Authenticator app

Number of days:

7

14

30

60

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Box 2: 14

Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in> <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure>

**NEW QUESTION 266**

.....



## Relate Links

**100% Pass Your MS-102 Exam with Examible Prep Materials**

<https://www.exambible.com/MS-102-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>