

# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam



### NEW QUESTION 1

- (Exam Topic 1)

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

NOTE: Each correct selection is worth one point.

Seattle:

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

New York:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

References:

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

### NEW QUESTION 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)

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

What is the minimum of dedicated support technicians required?

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

**Answer:** B

#### Explanation:

References:

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

### NEW QUESTION 4

- (Exam Topic 1)

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

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

NOTE: Each correct selection is worth one point.

New	Conditions	Device state (preview)
<p><b>Info</b></p> <p>Name: Policy1</p> <p><b>Assignments</b></p> <p>Users and groups: 0 users and groups selected</p> <p>Cloud apps: 1 app included</p> <p>Conditions: 0 conditions selected</p> <p><b>Access controls</b></p> <p>Grant: Block access</p> <p>Session: 0 controls selected</p> <p><b>Enable policy</b></p> <p>On Off</p>	<p><b>Info</b></p> <p>Sign-in risk: Not configured</p> <p>Device platforms: Not configured</p> <p>Locations: Not configured</p> <p>Client apps (preview): Not configured</p> <p>Device state (preview): Not configured</p>	<p><b>Info</b></p> <p>Configure: Yes No</p> <p>Include Exclude</p> <p>Select the device state condition used to exclude devices from policy.</p> <p><input type="checkbox"/> Device Hybrid Azure AD joined</p> <p><input type="checkbox"/> Device marked as compliant</p>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Suggested Answer

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

**NEW QUESTION 5**

- (Exam Topic 1)

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

What should you create from the Intune admin center?

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

**Answer:** C

**NEW QUESTION 6**

- (Exam Topic 4)

You are evaluating the required processes for Project1.

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

- A. host (A)
- B. host information
- C. text (TXT)
- D. pointer (PTR)

**Answer:** A

**Explanation:**

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

Note:

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

Mail exchanger (MX)

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

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

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

**NEW QUESTION 7**

- (Exam Topic 4)

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

Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication

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

**Answer:** C

**Explanation:**

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

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

Fabrikam does NOT plan to implement identity federation.

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

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

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

Reference:

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

**NEW QUESTION 8**

- (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 9**

- (Exam Topic 5)

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

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

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

**Answer:** A

**NEW QUESTION 10**

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

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

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

Actions

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

Answer Area

Device1: 

Action

Device2: 

Action

Device3: 

Action

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Actions

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

Answer Area

Device1: 

Disable BitLocker.

Device2: 

Switch to UEFI.

Device3: 

Upgrade to Windows 10 Enterprise.

**NEW QUESTION 10**

- (Exam Topic 5)  
 You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.  
 You plan to use Endpoint analytics to identify hardware issues.  
 You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

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

**Answer:** B

**NEW QUESTION 11**

- (Exam Topic 5)  
 HOTSPOT  
 Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription. The domain contains the users shown in the following table.

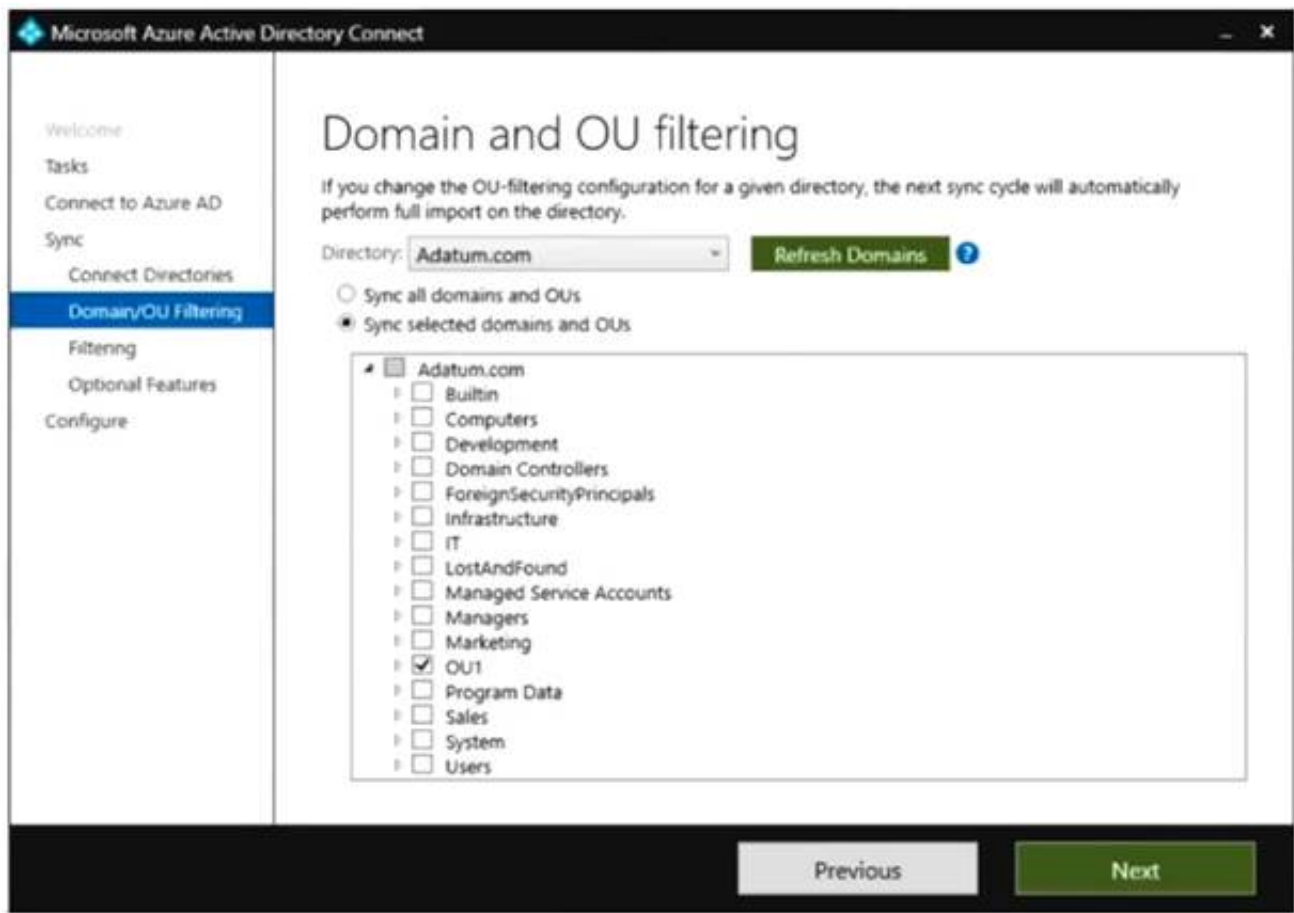
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.  
 You configure Domain and OU filtering as shown in the following exhibit.





You configure Filter users and devices as shown in the following exhibit.



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

**Answer Area**

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 syncs to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>
Group2 syncs to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 syncs to Azure AD.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group2 syncs to Azure AD.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

NEW QUESTION 15

- (Exam Topic 5)  
You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

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

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

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

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 17

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

- Identify when a user's credentials are compromised and shared on the dark web.
- Provide users that have compromised credentials with the ability to self-remediate. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

To identify when users have compromised credentials, configure:

▼

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

To enable self-remediation, select:

▼

Generate a temporary password

Require multi-factor authentication

Require password change

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web. User risk-based Conditional Access policy

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

Block access

Allow access but require a secure password change.

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

Box 2: Require password change

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

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

Reference:

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

**NEW QUESTION 20**

- (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 25**

- (Exam Topic 5)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

- A. Yes
- B. No

**Answer: B**

**Explanation:**

You need to assign the Security Administrator role. Reference:

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

**NEW QUESTION 29**

- (Exam Topic 5)



**HOTSPOT**

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

\* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.

Box 2: Yes.

\* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.

Box 3: No.

IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

Reference:

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

**NEW QUESTION 30**

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

- A. Yes
- B. No

**Answer:** A

### Explanation:

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

## NEW QUESTION 34

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.

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

**Answer Area**

Save the audit logs to:

Azure Active Directory admin center blade to use to view the saved audit logs:

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

**Answer Area**

Save the audit logs to:

Azure Active Directory admin center blade to use to view the saved audit logs:

## NEW QUESTION 38

- (Exam Topic 5)

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

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

Which users will receive the weekly digest email automatically?

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

Answer: E

Explanation:

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

NEW QUESTION 39

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune. You create an Android app protection policy named Policy1 that is targeted to all Microsoft apps and assigned to all users. Policy1 has the Data protection settings shown in the following exhibit.

Select apps to exempt

Select

Save copies of org data ⓘ

AllowBlock

Allow user to save copies to selected services ⓘ

SharePoint▼

Transfer telecommunication data to ⓘ

Any Dialer App▼

Dialer App Package ID

Dialer App Name

Received data from other apps ⓘ

All Apps▼

Open data into Org documents ⓘ

AllowBlock

Allow users to open data from services ⓘ

3 selected▼

Restrict cut, copy, and paste between other apps ⓘ

Policy managed apps with paste in▼

Cut and copy character limit for any app

0

Screen capture and Google Assistant ⓘ

AllowBlock

Approved keyboards ⓘ

RequireNot required

Select keyboards to approve

Select

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

Answer Area

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

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

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

▼  
any app  
only managed apps  
only unmanaged apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

OneDrive

local storage

Microsoft SharePoint Online

Microsoft SharePoint Online and OneDrive

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

any app

only managed apps

only unmanaged apps

NEW QUESTION 42

- (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 45

- (Exam Topic 5)  
HOTSPOT  
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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

Settings > Endpoints > computer1



computer1

Device summary

Risk level ⓘ

None

Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

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

Computer1 will be a member of [answer choice].

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

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

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped devices



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Group3 and Group4 only Computer1 has no Demo Tag.  
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 46

- (Exam Topic 5)  
HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he 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 less prevention (DLP) policy names 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 Policy' is applied to answer, selected 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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
**Answer Area**

User1: 

1

2

3

4

5

User2: 

1

2

3

4

5

**NEW QUESTION 47**

- (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: 

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Recent Microsoft service issues: 

Microsoft Secure Score

Adoption Score

Service health

Usage reports

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

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

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

Box 2: Service Health

Recent Microsoft service issues

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

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 52**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant

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

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

NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Choose locations to apply the policy

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

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

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

NEW QUESTION 54

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action. To which location can the policy be applied?

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

Answer: B

NEW QUESTION 59

- (Exam Topic 5)

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

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

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

Answer: A

Explanation:

Reference:

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

#### NEW QUESTION 61

- (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:

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

- 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 63

- (Exam Topic 5)

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

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours. You plan to sync contoso.com to an Azure AD tenant.

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

What should you include in the recommendation?

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

**Answer: A**

#### Explanation:

Reference:

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

#### NEW QUESTION 65

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen. Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Graphical user interface, text, application, chat or text message Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

NEW QUESTION 67

- (Exam Topic 5)  
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

SharePoint Content\_Export

Restart report

Download report

Delete

**Status:**  
The export has completed. You can start downloading the results.

**Items included from the search:**  
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

**Exchange content format:**  
One PST file for each mailbox.

**De-duplication for Exchange content:**  
Not enabled.

**SharePoint document versions:**  
Included

**Export files in a compressed (zipped) folder:**  
Yes

**The export data was prepared within region:**  
Default region

Close

Feedback

What will be excluded from the export?

- A. a 10-MB XLSX file
- B. a 5-MB MP3 file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file



visit - <https://www.surepassexam.com>



#### Answer Area

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

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

Graphical user interface, text, application Description automatically generated

#### NEW QUESTION 78

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users. What is the longest time range that can be included in the report?

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

**Answer:** C

#### Explanation:

View email security reports in the Microsoft 365 Defender portal

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

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

#### NEW QUESTION 82

- (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 87

- (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 91

- (Exam Topic 5)

HOTSPOT

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

Name	Role
User1	Global admin
User2	<i>None</i>
User3	<i>None</i>

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

Name	Role
User1	<i>None</i>
User2	Purchaser
User3	Basic Purchaser

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

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

**Answer:** A

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

**NEW QUESTION 95**

- (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	<b>None</b>
User2	Defender for Identity Contoso Users	<b>None</b>
User3	<b>None</b>	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

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

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 100**

- (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 bated on: When items were created  
 You need to prevent the removal of the label once the label K applied to a lie 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 105**

- (Exam Topic 5)

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

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

The tenant contains the devices shown in the following table.

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

**NEW QUESTION 110**

- (Exam Topic 5)

You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel. What should you do in the Cloud App Security admin center?

- A. From Automatic log upload, add a log collector.
- B. From Automatic log upload, add a data source.
- C. From Connected apps, add an app connector.
- D. From Security extension, add a SIEM agent.

**Answer:** D

**NEW QUESTION 111**

- (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:

User2:

- 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 112**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

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

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

**Answer:** D

**NEW QUESTION 117**

- (Exam Topic 5)

HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

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

You have the apps shown in the following table.

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

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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

NOTE: Each correct selection is worth one point.



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

- A. Mastered  
 B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy> <https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>

**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.

You have a computer that runs Windows 10.

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

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

Does this meet the goal?

- A. Yes  
 B. No

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 123**

- (Exam Topic 5)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.



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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Graphical user interface, text, application Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

NEW QUESTION 124

- (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 125

- (Exam Topic 5)  
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.  
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

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

Users may register their devices with Azure AD ⓘ

All

None

[Learn more on how this setting works](#)

Require Multi-Factor Auth to join devices ⓘ

Yes

No

Maximum number of devices per user ⓘ

5

▼

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 127

- (Exam Topic 5)

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.  
The Products & services settings in Microsoft Store for Business are shown in the following exhibit.

**Microsoft Remote Desktop**  
Free • Online • [Product Details](#)

Install

Licenses

Unlimited licenses  
0 used

Billing

€0.00 (Free app)

Settings & Actions

Not in private store  
[More actions available on details page](#)

**Excel Mobile**  
Free • Online • [Product Details](#)

Install

Licenses

Unlimited licenses  
0 used

Billing

€0.00 (Free app)

Settings & Actions

In private store  
[More actions available on details page](#)

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
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated

Reference:

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

**NEW QUESTION 130**

- (Exam Topic 5)

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

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 134**

- (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 135**

- (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 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Endpoint Management admin center, you create a device configuration profile. Does this meet the goal?

- A. Yes  
 B. No

**Answer:** B

**Explanation:**

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

**NEW QUESTION 140**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

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

- A. Microsoft Exchange Online only
- B. Microsoft Teams only
- C. Microsoft Exchange Online and SharePoint Online only
- D. Microsoft Teams and SharePoint Online only
- E. Microsoft Teams, Exchange Online, and SharePoint Online

**Answer:** A

**Explanation:**

Privileged access management

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

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

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

**NEW QUESTION 141**

- (Exam Topic 5)

**HOTSPOT**

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

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

The devices are configured as shown in the following table.

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

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

\* 1. Assignments

- > Users or workload identities: Group1
- > Cloud apps or actions: Office 365 SharePoint Online
- > Conditions

- Filter for devices: Exclude filtered devices from the policy

- Rule syntax: device.displayName -startsWith "Device"

\* 2. Access controls

- > Grant
- Grant: Block access
- > Session: 0 controls selected

\* 3. Enable policy: On

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

User1 is member of Group1 and has Device1. Device1 is not Azure AD joined.

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

Box 2: Yes

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

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

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

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

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



certificate before they can continue to use the browser.  
Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join>  
<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-com>

**NEW QUESTION 142**

- (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?

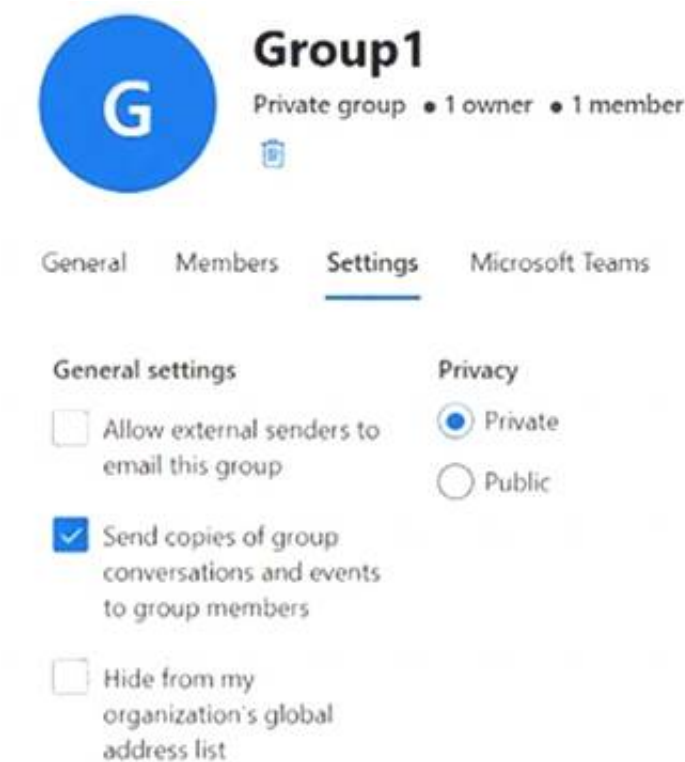
- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**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 146**

- (Exam Topic 5)  
HOTSPOT  
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



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



**Answer Area**

Action:

Portal:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Invite User1 to collaborate with your organization as a guest.  
 To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps. Navigate with your Web browser to <https://admin.microsoft.com>.  
 On the left pane, click on “Users”, then click “Guest Users”.  
 On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user” link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.  
 On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.  
 Box 2: The Microsoft Entra admin center  
 Microsoft Entra admin center unites Azure AD with family of identity and access products  
 Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.  
 Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).  
 Reference:  
<https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users> <https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-ac>

**NEW QUESTION 150**  
 - (Exam Topic 5)  
 HOTSPOT

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

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

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

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

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

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

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

Answer Area

Statements

- If a high-severity incident is triggered for Device1, an incident email notification will be sent.
- If a low-severity incident is triggered for Computer1, an incident notification email will be sent.
- If a low-severity incident is triggered for Device3, an incident notification email will be sent.

Yes	No
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No  
Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No  
Computer1 does not belong to either Group1 or Group2

Box 3: Yes  
Device3 belongs to both Group1 and Group2. Note: Understanding alert severity  
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.  
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.  
Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue>

NEW QUESTION 152



- (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 153


- (Exam Topic 5)
- HOTSPOT
- You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.


Custom smart lockout

Lockout threshold  15 

Lockout duration in seconds  600 

Custom banned passwords

Enforce custom list  Yes No

Custom banned password list 

3hundred


Eleven


Falcon

Project

Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory  Yes No

Mode  Enforced Audit

- User1 attempts to update their password to the following passwords:
- > F@lcon
  - > Project22
  - > T4il\$pin45dg4
- Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
- NOTE: Each correct selection is worth one point.

**Answer Area**

[Answer choice] will be accepted as a password.

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

Only T4il\$pin45dg4
Only F@lcon and T4il\$pin45dg4
Only Project22 and T4il\$pin45dg4
F@lcon, Project22, and T4il\$pin45dg4

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Only T4il\$pin45dg4

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

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

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

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

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

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

**NEW QUESTION 155**

- (Exam Topic 5)

Your company has a Microsoft 365 E5 subscription. Users in the research department work with sensitive data.

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

Users in other departments must not be restricted.

What should you do?

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

**Answer:** D

**Explanation:**

Use the Microsoft 365 Defender portal to create Safe Links policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies

& Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinksv2>.

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

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

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

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

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

\*-> Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).

The specified Microsoft 365 Groups.

Domains: All recipients in the specified accepted domains in your organization. Etc.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>

**NEW QUESTION 157**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

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

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

**Answer:** C



#### Explanation:

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

Specific types of sensitive information.

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

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

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels)

Teams chats

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

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

#### NEW QUESTION 158

- (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 161

- (Exam Topic 5)

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings: > Show app and profile configuration progress: Yes

> Allow users to collect logs about installation errors: Yes

> Assignments: Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

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

#### NEW QUESTION 166



- (Exam Topic 5)  
DRAG DROP

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

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

You use Azure Information Protection.  
You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Authorize Server1.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run GenConnectorConfig.ps1 on Server1.

Run GenConnectorConfig.ps1 on Server2.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Reference:  
<https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector> <https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector>

NEW QUESTION 170

- (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 174

- (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 177

- (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 upgrade Server1 to Windows Server 2019.  
 Does this meet the goal?

- A. yes
- B. No

**Answer:** A

**NEW QUESTION 178**

- (Exam Topic 5)  
 You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.  
 You need to prevent the members of Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.  
 What should you use?

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

**Answer:** A

**NEW QUESTION 179**

- (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 182

- (Exam Topic 5)  
HOTSPOT

You have a Microsoft 365 subscription.  
You deploy the anti-phishing policy shown in the following exhibit.  
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

Answer Area

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

Add trusted senders and domains

Enable domains to protect

Enable users to protect

Phishing email threshold

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

Add trusted senders and domains

Enable intelligence for impersonation protection

Enable spoof intelligence

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Enable users to protect  
Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.  
User impersonation protection  
User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.  
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).  
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.  
Box 2: Add trusted senders and domains  
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.  
Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

NEW QUESTION 186

- (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 189**

- (Exam Topic 5)

HOTSPOT

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

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

All the groups are deleted.

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

NOTE: Each correct selection is worth one point.

Groups that can be restored:

Group3 only

Group1 and Group2 only

Group2 and Group4 only

Group1, Group2, and Group3 only

Group1, Group2, Group3, and Group4

Retention period:

24 hours

7 days

14 days

30 days

90 days

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Group3 only Box 2: 30 days

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a

"soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/restore-deleted-group>

**NEW QUESTION 192**

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### MS-102 Practice Exam Features:

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

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