

# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam



**NEW QUESTION 1**

HOTSPOT - (Topic 6)

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

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

The tenant contains the devices shown in the following table.

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

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

Statements	Yes	No
Device1 is marked as compliant.	<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:**

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

**NEW QUESTION 2**

- (Topic 6)

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

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

The solution must use the principle of least privilege.

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 3**

DRAG DROP - (Topic 6)  
 DRAG DROP

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

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

The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Roles**

- Billing Administrator
- Global Administrator
- Helpdesk Administrator
- License Administrator
- Service Support Administrator
- User Administrator

**Answer Area**

Group1:

Group2:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Billing admin manage service request Purchase new services Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

**NEW QUESTION 4**

HOTSPOT - (Topic 6)  
 HOTSPOT

You have a Microsoft 365 subscription.

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

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

## Answer Area



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Usage reports

The daily active users in Microsoft Teams

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

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

Box 2: Service Health

Recent Microsoft service issues

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

### NEW QUESTION 5

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to assign the Security Administrator role. Reference:

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

### NEW QUESTION 6

- (Topic 6)

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

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

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

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

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

? Administrative effort must be minimized.

What should you include in the recommendation?

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

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 7

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

? Report on shared documents that contain PII.

What should you create?

- A. an alert policy
- B. a data loss prevention (DLP) policy
- C. a retention policy
- D. a Microsoft Cloud App Security policy

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 8

- (Topic 6)

You have a Microsoft 365 subscription.

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

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### NEW QUESTION 9

- (Topic 6)

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

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

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

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

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

**Answer: B**

#### Explanation:

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

Reference:

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

#### NEW QUESTION 10

- (Topic 6)

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

#### NEW QUESTION 10

- (Topic 6)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
 You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.  
 Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.  
 Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 15**

- (Topic 6)

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-authentication>

**NEW QUESTION 17**

- (Topic 6)

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

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

You configure Azure AD Connect to sync contoso.com to Azure AD.

Which objects will sync to Azure AD?

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

**Answer: D**

**Explanation:**

Disabled accounts

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

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

**NEW QUESTION 20**

HOTSPOT - (Topic 6)

HOTSPOT

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

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

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can

modify the setting. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

User:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Microsoft 365 setting:

- Office installation options
- Privileged access
- Release preferences

User:

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

**NEW QUESTION 24**

HOTSPOT - (Topic 6)

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 29**

- (Topic 6)

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

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

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The question states that “all the user account synchronizations completed successfully”. Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

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

**NEW QUESTION 34**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.

All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.

You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

✕

## New audit retention policy

**Name \***

**Description**

**Record Types**

**Activities**

**Users:**

**Duration \*:**

90 Days

6 Months

1 Year

**Priority \*:**

After Policy1 is created, the following actions are performed:

- ? Admin1 creates a user named User1.
- ? Admin2 creates a user named User2.

How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1: 

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2: 

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

User1: 

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2: 

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

**NEW QUESTION 38**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

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

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

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

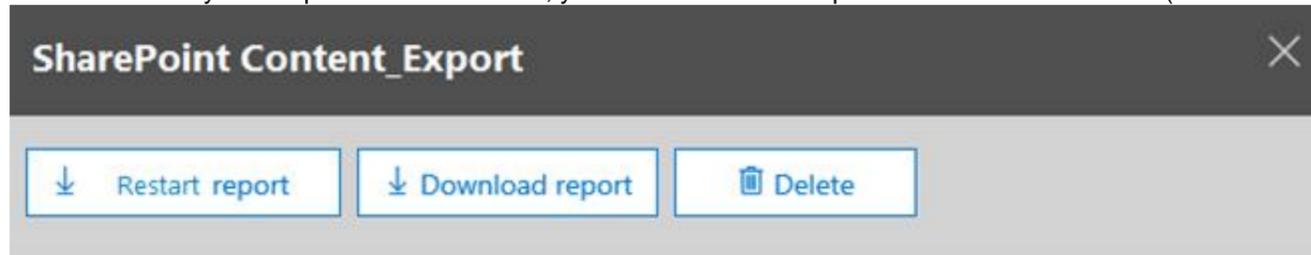
- A. anonymous IP address only
- B. anonymous IP address and atypical travel
- C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
- D. unfamiliar sign-in properties and atypical travel only
- E. anonymous IP address and unfamiliar sign-in properties only

**Answer:** C

**NEW QUESTION 41**

- (Topic 6)

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



**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

**Answer: B**

**Explanation:**

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

**NEW QUESTION 46**

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

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

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**NEW QUESTION 50**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations.

What should you use?

- A. Microsoft Purview
- B. Azure AD Identity Protection
- C. Microsoft Secure Score
- D. the configuration analyzer

**Answer: C**

**NEW QUESTION 51**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

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

You need to prevent the removal of the label once the label is applied to 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 52**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

**Review your settings**

**Name** Edit

Retention1

**Description for admins** Edit

**Description for users** Edit

**File plan descriptors** Edit

Reference Id: 1

Business function/department Legal

Category: Compliance

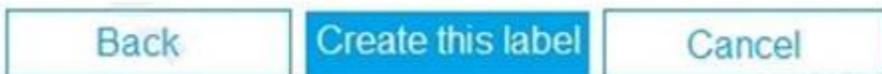
Authority type: Legal

**Retention** Edit

7 years

Retain only

Based on when it was created



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

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

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 55**

- (Topic 6)

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed. What should you do on the computer?

- A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
- B. install the West feature update and the latest quality update only.
- C. install all the feature updates released since version 2004 and the latest quality update only.
- D. install the latest feature update and all the quality updates released since version 2004.

**Answer: B**

**NEW QUESTION 58**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

```

-Scopes User.ReadWrite.All, Organization.Read.All
Connect-AzureAD
Connect-MgGraph
Connect-MSOLService

$E3 = Get-MgSubscribedSku | Where SkuPartNumber -eq 'EnterprisePack'

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in ("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$licenseOptions= @(
    @(
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    )
)

Set-MgUserLicense -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
    
```

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

```
Set-MgUserLicense -UserId $userUPN -AddLicenses @{$Skuld = "<Skuld>"} - RemoveLicenses @()
```

This example assigns a license from the SPE\_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
```

```
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{$Skuld =
```

```
$e5Sku.Skuld} -RemoveLicenses @()
```

**NEW QUESTION 59**

- (Topic 6)

You have a Microsoft 365 subscription.

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

What should you do?

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

**Answer: A**

**NEW QUESTION 63**

- (Topic 6)

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 68**

- (Topic 6)

You have a Microsoft E5 subscription.

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

What should you implement?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 73**

HOTSPOT - (Topic 6)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Reset the password of User4: User1 and User3 only

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

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

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

**NEW QUESTION 77**

HOTSPOT - (Topic 6)  
 HOTSPOT

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

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

The forest contains the users shown in the following table.

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

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

**PROVISION FROM ACTIVE DIRECTORY**



**Azure AD Connect cloud provisioning**

This feature allows you to manage provisioning from the cloud.

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

**Azure AD Connect sync**

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

**USER SIGN-IN**



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

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

Answer Area

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

**NEW QUESTION 80**

- (Topic 6)

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

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

Which properties of the alerts can you modify?

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 83**

HOTSPOT - (Topic 6)

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

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

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes  No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

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

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

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

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

**NEW QUESTION 88**

DRAG DROP - (Topic 6)

Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level

of medium or lower to access Microsoft Exchange Online mailboxes.

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

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solutions	Answer Area
An app configuration policy	Company-owned devices: Solution
An app protection policy	Personal devices: Solution
A compliance policy	
A configuration profile	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Solutions	Answer Area
An app configuration policy	Company-owned devices: A compliance policy
An app protection policy	Personal devices: An app protection policy
A compliance policy	
A configuration profile	

**NEW QUESTION 92**

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

What should you do first?

- A. Delete the workspace.
- B. Create a workspace.
- C. Onboard a new device.
- D. Offboard the test devices.

**Answer:** B

**Explanation:**

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

\* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data- workspace>

**NEW QUESTION 95**

- (Topic 6)

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

You install and register the network scanner on a device named Device1.

What should you do next?

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

**Answer:** C

**NEW QUESTION 96**

- (Topic 6)

You have a Microsoft 365 subscription.

You view the Service health Overview as shown in the following exhibit.

## Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

Report an issue Customize

### Active issues

Issue title	Affected service	Issue type
Microsoft service health (6)		
Issues in your environment that require action (0)		

### Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	3 advisories
Microsoft 365 suite	2 advisories
Microsoft Teams	1 advisory
OneDrive for Business	1 advisory
SharePoint Online	2 advisories

You need to ensure that a user named User1 can view the advisories to investigate service health issues. Which role should you assign to User1?

- A. Message Center Reader
- B. Reports Reader
- C. Service Support Administrator
- D. Compliance Administrator

**Answer: B**

**Explanation:**

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

Incorrect:

\* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups

\* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

**NEW QUESTION 100**

**HOTSPOT - (Topic 6)**

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy. You need to identify the following information:

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

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

**Answer Area**

To identify the number of emails quarantined by ZAP:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

To identify the number of emails quarantined by ZAP:

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

**NEW QUESTION 104**

**HOTSPOT - (Topic 6)**

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

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

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

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

**Microsoft Authenticator settings**

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

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

**Enable and Target**    Configure

Enable

Include    Exclude

Target  All users     Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

**NEW QUESTION 105**

- (Topic 6)

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

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

Answer: A

**NEW QUESTION 108**

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Role
User1	Global admin
User2	None
User3	None

You provision the private store in Microsoft Store for Business.

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

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business. Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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

**NEW QUESTION 110**

- (Topic 6)

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

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

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

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

**Answer:** E

**NEW QUESTION 114**

- (Topic 6)

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 116**

- (Topic 6)

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

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

Your network contains an Active Directory domain. You deploy a Microsoft Entra tenant.

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

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

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

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

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

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 118**

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	<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 AD join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 123**

HOTSPOT - (Topic 6)

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:

Number of days:

- 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.

**NEW QUESTION 126**

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 130**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

Industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard.

- A. From Policy in the Azure portal, select Compliance, and then assign a policy.
- B. From Compliance Manager, create an assessment.
- C. From the Microsoft 365 compliance center, create an audit retention policy.
- D. From the Microsoft 365 admin center, enable the Productivity Score.

**Answer:** B

**NEW QUESTION 135**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint.

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

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

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

**Answer:** AC

**NEW QUESTION 137**

- (Topic 6)

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site. What should you do?

- A. From the SharePoint Online site, create an alert.
- B. From the SharePoint Online admin center, modify the sharing settings.
- C. From the Microsoft 365 Defender portal, create an alert policy.
- D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

**Answer:** D

**NEW QUESTION 139**

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

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

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

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

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

**Answer Area**

**Statements**

	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	<input type="checkbox"/>	<input type="checkbox"/>
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: No  
 Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.  
 Box 2: No  
 Computer1 does not belong to either Group1 or Group2  
 Box 3: Yes  
 Device3 belongs to both Group1 and Group2.  
 Note: Understanding alert severity  
 Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.  
 The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

**NEW QUESTION 140**

- (Topic 6)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 145**

- (Topic 6)

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

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

Your network contains an Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.

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

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

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

- A. Yes
- B. No

**Answer: A**

**NEW QUESTION 148**

- (Topic 6)

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

All the devices in your organization are onboarded to Microsoft Defender for Endpoint.

You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

What should you do?

- A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
- B. From Alerts queue, create a suppression rule and assign an alert.
- C. From Advanced hunting, create a query and a detection rule.
- D. From the Microsoft Purview compliance portal, create an audit log search.

**Answer: C**

**NEW QUESTION 150**

- (Topic 6)

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

**Answer: B**

**Explanation:**

Reference:

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

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

**NEW QUESTION 151**

- (Topic 6)

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

### Azure AD Connect sync

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

## USER SIGN-IN



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

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

- A. Yes
- B. No

**Answer:** A

### Explanation:

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

## NEW QUESTION 155

- (Topic 6)

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-1-now-included-in-m365-e3/ba-p/3060639>

**NEW QUESTION 159**

- (Topic 6)

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

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

Where can you store data from the LinkedIn connector?

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 164**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

**Answer Area**

**Policies**

- Anti-phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links

**Rules**

- Tenant Allow/Block Lists
- Email authentication settings
- DKIM
- Advanced delivery
- Enhanced filtering
- Quarantine policies

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 167**

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 171**

HOTSPOT - (Topic 6)

HOTSPOT

				actions				
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 172**

- (Topic 6)

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

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

Which users will receive the weekly digest email automatically?

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

**Answer: E**

**Explanation:**

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

**NEW QUESTION 177**

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

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

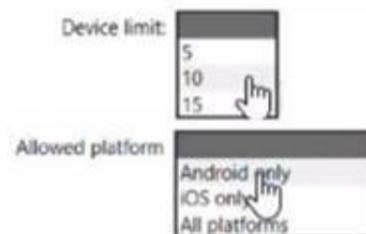
The device type restriction are configured as shown in the following table.

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

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

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

**Answer Area**



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 182**

- (Topic 6)

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

After you answer a question in this section, you will NOT be able to return to it as a result, these questions will not appear in the review screen.  
 Your network contains an Active Directory domain. You deploy an Azure AD tenant.  
 Another administrator configures the domain to synchronize to Azure AD.  
 You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.  
 You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.  
 You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings.  
 Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**NEW QUESTION 186**

DRAG DROP - (Topic 6)

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.  
 All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.  
 You plan to implement self-service password reset (SSPR).  
 You need to ensure that when a user resets or changes a password, the password syncs with AD DS.  
 Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
 NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 190**

- (Topic 6)

You have a Microsoft 365 E5 subscription.  
 You create an account for a new security administrator named SecAdmin1.  
 You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.  
 Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.  
 Does this meet the goal?

- A. Yes
- B. no

**Answer: B**

**NEW QUESTION 194**

HOTSPOT - (Topic 6)

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

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

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in The answer area.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Computer1:  Group1 only  
 Group1 only  
 Group2 only  
 Group1 and Group2  
 Ungrouped devices

Computer2:  Group1 only  
 Group1 only  
 Group3 only  
 Group1 and Group3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Computer1:  Group1 only  
 Group1 only  
 Group2 only  
 Group1 and Group2  
 Ungrouped devices

Computer2:  Group1 only  
 Group1 only  
 Group3 only  
 Group1 and Group3

**NEW QUESTION 197**

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

**Answer:** A

**Explanation:**

Privileged access management

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

Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

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

Reference:

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

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

**NEW QUESTION 199**

- (Topic 6)

You have a Microsoft 365 E5 subscription. You need to create a mail-enabled contact. Which portal should you use?

- A. the Microsoft 365 admin center
- B. the SharePoint admin center
- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

**Answer: A**

**NEW QUESTION 204**

- (Topic 6)

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

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

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

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

**Answer: A**

**NEW QUESTION 207**

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

**Answer: C**

**Explanation:**

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

Reference:

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

**NEW QUESTION 212**

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

- A. Security Reader
- B. Global Administrator
- C. Owner
- D. User Administrator

**Answer: A**

**NEW QUESTION 213**

HOTSPOT - (Topic 6)

HOTSPOT

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

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

The devices are configured as shown in the following table.

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

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

? Users or workload identities: Group1

? Cloud apps or actions: Office 365 SharePoint Online

? Conditions

- Filter for devices: Exclude filtered devices from the policy

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

? Grant

- Grant: Block access

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

**Statements**

**Yes**

**No**

User1 can access Site1 from Device1.



User2 can access Site1 from Device2.



User2 can access Site1 from Device3.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

User1 is member of Group1 and has Device1.

Device1 is not Azure AD joined.

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

Box 2: Yes

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

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

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

Device3 is Android and is Azure AD registered.

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

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

**NEW QUESTION 217**

HOTSPOT - (Topic 6)

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

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File1:    
 Tip2 only   
 Tip3 only   
 Tip2 and Tip3

File2:    
 Tip1 only   
 Tip3 only   
 Tip1 and Tip2 only   
 Tip1, Tip2, and Tip3

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

File1:    
 Tip2 only   
 Tip3 only   
 Tip2 and Tip3

File2:    
 Tip1 only   
 Tip3 only   
 Tip1 and Tip2 only   
 Tip1, Tip2, and Tip3

**NEW QUESTION 221**

DRAG DROP - (Topic 6)

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

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

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

NOTE: Each correct selection is worth one point.

<p><b>Policy Types</b></p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">App configuration policy</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">App protection policy</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Compliance policy</div> <div style="border: 1px solid gray; padding: 2px;">Conditional Access policy</div>	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;">•</div> <div style="margin-bottom: 10px;">•</div> <div style="margin-bottom: 10px;">•</div> <div style="margin-bottom: 10px;">•</div> </div>	<p><b>Answer Area</b></p> <p>Device1: <input style="width: 100px;" type="text"/></p> <p>Device2: <input style="width: 100px;" type="text"/></p> <p>Device3: <input style="width: 100px;" type="text"/></p>
---	--	--

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Policy Types**

- App configuration policy
- App protection policy
- Compliance policy
- Conditional Access policy

**Answer Area**

- Device1: App protection policy
- Device2: Conditional Access policy
- Device3: Compliance policy

**NEW QUESTION 225**

- (Topic 6)

You have a Microsoft 365 subscription that uses Security & Compliance retention policies. You implement a preservation lock on a retention policy that is assigned to all executive users. Which two actions can you perform on the retention policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point?

- A. Add locations to the policy
- B. Reduce the duration of policy
- C. Remove locations from the policy
- D. Extend the duration of the policy
- E. Disable the policy

**Answer: AB**

**NEW QUESTION 230**

DRAG DROP - (Topic 6)

Your company has an Azure AD tenant named contoso.onmicrosoft.com. You purchase a domain named contoso.com from a registrar and add all the required DNS records. You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com. You need to configure User1 to sign in as user1@contoso.com. 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
Run update-igdomain -domainid contoso.com.	➔	<div style="border: 1px dashed gray; padding: 10px; margin: 0 auto; width: 80%;"> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Add a custom domain name.</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Verify the custom domain.</div> <div style="border: 1px solid gray; padding: 5px;">Modify the username of User1.</div> </div>
Modify the email address of User1.	➔	
Add contoso.com as a SAN for an X.509 certificate.	➔	
Add a custom domain name.	➔	
Verify the custom domain.	➔	
Modify the username of User1.	➔	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Actions		Answer Area
Run update-igdomain -domainid contoso.com.	➔	<div style="border: 1px dashed gray; padding: 10px; margin: 0 auto; width: 80%;"> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Add a custom domain name.</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Verify the custom domain.</div> <div style="border: 1px solid gray; padding: 5px;">Modify the username of User1.</div> </div>
Modify the email address of User1.	➔	
Add contoso.com as a SAN for an X.509 certificate.	➔	
Add a custom domain name.	➔	
Verify the custom domain.	➔	
Modify the username of User1.	➔	

**NEW QUESTION 234**

HOTSPOT - (Topic 6)

You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

```

Select Administrator: Windows PowerShell
Name           : Retention1
Priority        : 200
RecordTypes     : {MicrosoftTeams}
Operations      : {}
UserIds         : {}
RetentionDuration : ThreeMonths

Name           : Retention2
Priority        : 150
RecordTypes     : {MicrosoftTeams}
Operations      : {teamcreated}
UserIds         : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name           : Retention3
Priority        : 100
RecordTypes     : {}
Operations      : {}
UserIds         : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths

PS C:\>
    
```

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

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

**NEW QUESTION 239**

HOTSPOT - (Topic 6)

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.docx	2
File4.bmp	3
File5.doc	3

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.

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**

User 1:

User 2:

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

User 1:

User 2:

**NEW QUESTION 242**

DRAG DROP - (Topic 6)

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the

correct order.

**Actions**

**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:**

**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.



- From the Cloud App Security admin center, add an app connector.
- Create a conditional access policy.
- Sign in to App1.

**NEW QUESTION 244**

HOTSPOT - (Topic 6)

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

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

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

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

- Name: Notification
- Notification settings
  - o Notify on alert severity: Low. Medium
  - o Device group scope: DevtceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

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

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

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

**NEW QUESTION 246**

HOTSPOT - (Topic 6)  
 HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

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

You add the following assignment for the Exchange Administrator role:

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Admin1 is member of Group1.

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

July 15, 2023 is with the assignment period.

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

Box 2: No

Admin2 is member of Group2.

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

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

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

Box 3: Yes

Admin3 is member of Group1 and Group2.

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

May 1, 2023 is with the assignment period.

**NEW QUESTION 250**

DRAG DROP - (Topic 6)

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

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

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

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Onboarding method**

- 
- 
- 
- 
-

**Device Type**

Corporate:

BYOD:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Onboarding method**

- 
- 
- 
- 
-

**Device Type**

Corporate:

BYOD:

**NEW QUESTION 255**

HOTSPOT - (Topic 6)  
 HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

**NEW QUESTION 260**

- (Topic 6)

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

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

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

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

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

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

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

Reference:

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

**NEW QUESTION 261**

HOTSPOT - (Topic 6)

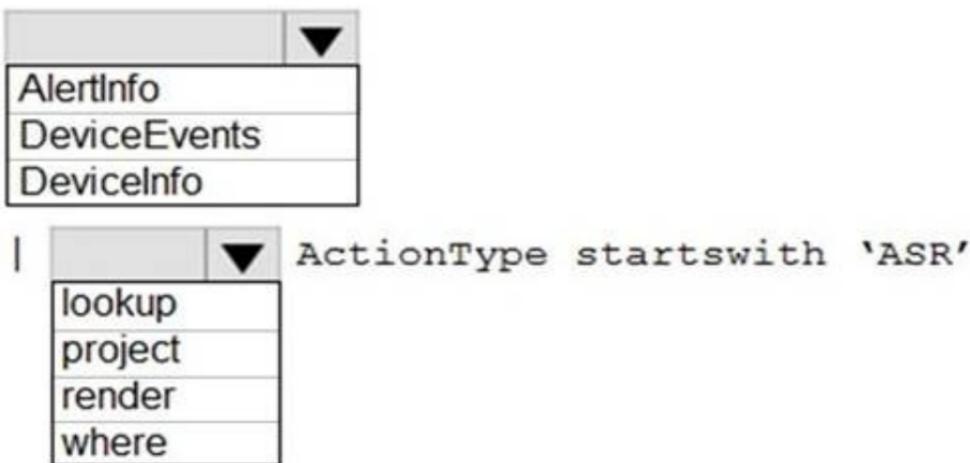
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

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.



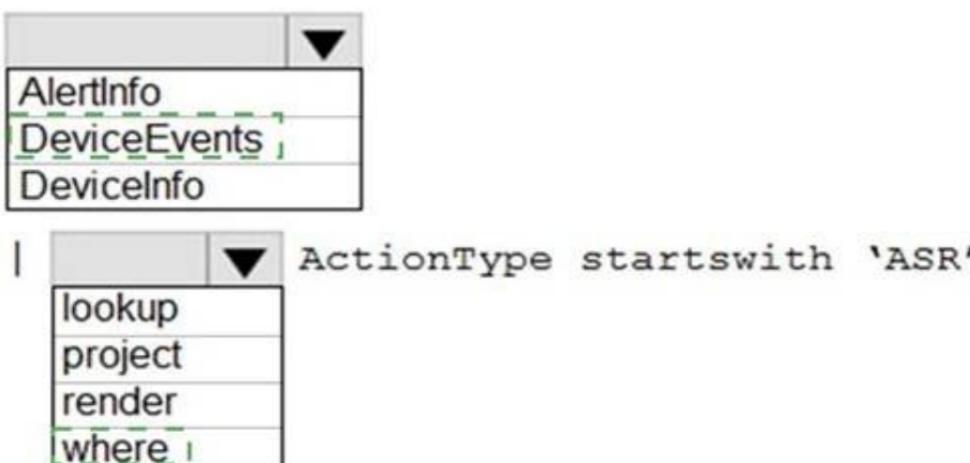
The screenshot shows a Kusto query editor. The first dropdown menu is open, showing the following options: AlertInfo, DeviceEvents, and DeviceInfo. The second dropdown menu is also open, showing the following options: lookup, project, render, and where. The text 'ActionType startswith 'ASR'' is visible next to the second dropdown menu.

A. Mastered

B. Not Mastered

**Answer: A**

**Explanation:**



The screenshot shows the Kusto query editor with the correct selections. In the first dropdown menu, 'DeviceEvents' is selected. In the second dropdown menu, 'where' is selected. The text 'ActionType startswith 'ASR'' is visible next to the second dropdown menu.

**NEW QUESTION 266**

HOTSPOT - (Topic 6)

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

# Domains

+ Add domain Buy domain Refresh

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

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

**Answer Area**

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

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

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

**NEW QUESTION 271**

**HOTSPOT - (Topic 6)**

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to identify the settings that are below the Standard protection profile settings in the preset security policies. What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Portal: Microsoft 365 Defender portal

Feature: Configuration analyzer

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Portal:

Feature:

**NEW QUESTION 272**

- (Topic 6)

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

Home > sensitivity

Labels Label policies Auto-labeling (preview)

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

+ Create a label Publish labels Refresh

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

Which labels can users apply to content?

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

**Answer: C**

**NEW QUESTION 276**

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

Settings > Endpoints > computer1



# computer1

## Device summary

Risk level ⓘ

None

## Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

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

**Answer Area**

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 277**

- (Topic 6)

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

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

You have a computer that runs Windows 10.

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

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 279**

- (Topic 6)

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

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

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

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

**Answer: B**

**NEW QUESTION 283**

- (Topic 6)

You have a Microsoft 365 subscription.

You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox. What should you configure?

- A. a data loss prevention (DLP) policy
- B. an alert policy
- C. an audit search
- D. an insider risk management policy

**Answer: B**

**NEW QUESTION 288**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected. What should you use to create the policy?

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

**Answer: C**

**NEW QUESTION 293**

HOTSPOT - (Topic 6)

Your company uses Microsoft Defender for Endpoint.

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

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 296

HOTSPOT - (Topic 6)

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 300**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

What should you configure?

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

**Answer:** B

**Explanation:**

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

Sign-in risk policy  
 User risk policy

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

Reference:

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

**NEW QUESTION 305**

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

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

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator 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>

**NEW QUESTION 307**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

Answer Area

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

Domains to protect

Domains to protect

Mailbox intelligence

Users to protect

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

Global settings for safe attachments

Global settings for safe attachments

The Safe Attachments policy settings

The Safe Links policy settings

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

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

Domains to protect

Domains to protect

Mailbox intelligence

Users to protect

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

Global settings for safe attachments

Global settings for safe attachments

The Safe Attachments policy settings

The Safe Links policy settings

**NEW QUESTION 310**

- (Topic 6)

: 241

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

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

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 312**

- (Topic 6)

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

? Microsoft Teams

? Microsoft OneDrive  
 ? Microsoft Exchange Online  
 ? Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

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

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

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 317**

- (Topic 6)

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

**PROVISION FROM ACTIVE DIRECTORY**



**Azure AD Connect cloud provisioning**

This feature allows you to manage provisioning from the cloud.

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

**Azure AD Connect sync**

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

**USER SIGN-IN**



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

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

Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2

could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

**NEW QUESTION 320**

HOTSPOT - (Topic 6)

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

? Only show page to devices provisioned by out-of-box experience (OOBE): No

? 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.

If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.

If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Statements**

**Yes No**

If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.

If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.

If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.

**NEW QUESTION 325**

- (Topic 6)

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

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

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

What should you do?

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

**Answer: B**

**NEW QUESTION 327**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

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

**Answer: D**

**NEW QUESTION 331**

- (Topic 6)

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

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

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

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

**Answer: D**

**Explanation:**

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

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

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

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

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

Password hash synchronization Pass-through authentication

Active Directory Federation Services

Reference:

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

**NEW QUESTION 334**

DRAG DROP - (Topic 6)

DRAG DROP

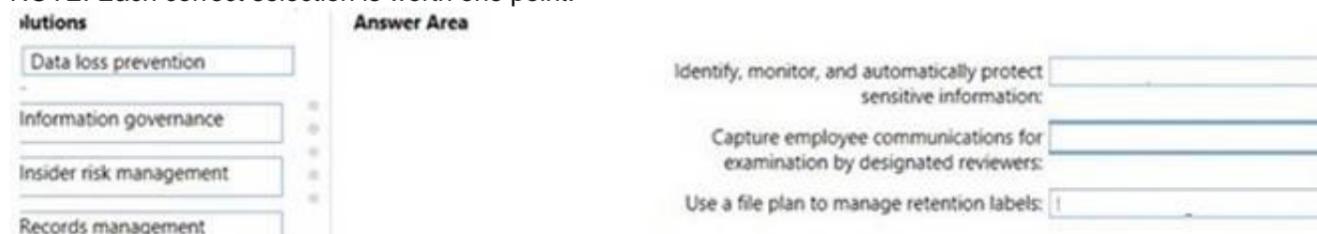
You have a Microsoft 365 E5 tenant.

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

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

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

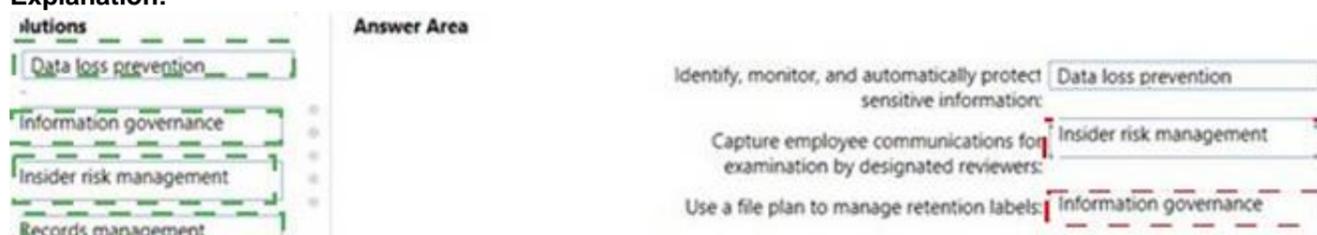
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 336**

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

What should you modify?

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

**Answer: C**

**NEW QUESTION 337**

HOTSPOT - (Topic 6)

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

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

**Windows 10 compliance policy**  
Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-do-date	Require	Not configured
Real-time protection	Require	Not configured

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

**Windows 10 compliance policy**  
Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-do-date	Require	Not configured
Real-time protection	Require	Not configured

**NEW QUESTION 340**

- (Topic 6)

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 342**

HOTSPOT - (Topic 6)

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

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

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

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

**Answer Area**

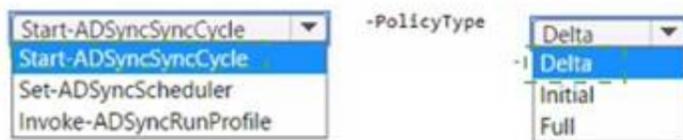


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 347**

- (Topic 6)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij.

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

D18912E1457D5D1DDCBD40AB3BF70D5D

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 351**

- (Topic 6)

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 352

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

**Answer:** A

#### Explanation:

Demonstrate data protection

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

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

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

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

? Click Data loss prevention > Policy.

? Click + Create a policy.

? In Start with a template or create a custom policy, click Custom > Custom policy > Next.

? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens

? Etc.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

#### NEW QUESTION 354

- (Topic 6)

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

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,

You enable device clean-up rules

What can you configure as the minimum number of days before a device is removed automatically?

- A. 10
- B. 30
- C. 45
- D. 90

**Answer:** D

#### NEW QUESTION 357

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

Which authentication method should you use?

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

**Answer:** C

#### NEW QUESTION 360

- (Topic 6)

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

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

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

What should you include in the recommendation?

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

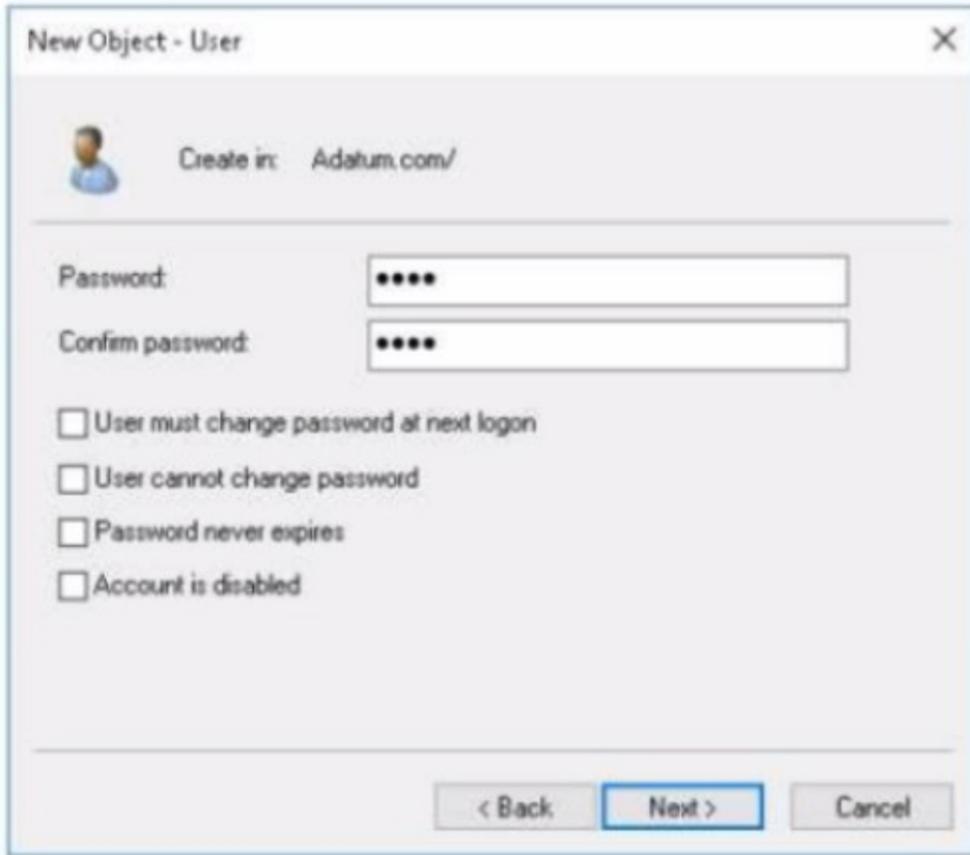
**Answer:** D

#### NEW QUESTION 363

**HOTSPOT - (Topic 6)**

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

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



The Azure AD password policy is configured as shown in the following exhibit. Password policy Set the password policy for all users in your organization. Days before passwords expire 90 Days before a user is notified about 14 expiration You confirm that User1 is synced to Azure AD. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

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

**NEW QUESTION 367**

**HOTSPOT - (Topic 6)**

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD). The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

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

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

? For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

? Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

**Statements**

**Yes No**

Establish a threat intelligence program will appear as Implemented in the SP800 assessment.

The SP800 assessment score will increase by 54 points.

The Data Protection Baseline score will increase by 9 points.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Statements**

**Yes No**

Establish a threat intelligence program will appear as Implemented in the SP800 assessment.

The SP800 assessment score will increase by 54 points.

The Data Protection Baseline score will increase by 9 points.

**NEW QUESTION 372**

- (Topic 6)

You purchase a new computer that has Windows 10, version 21H1 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

- A. Install all the feature updates released since version 21H1 and the latest quality update only.
- B. Install the latest feature update and all the quality updates released since version 21H1.
- C. Install the latest feature update and the latest quality update only.
- D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

**Answer:** C

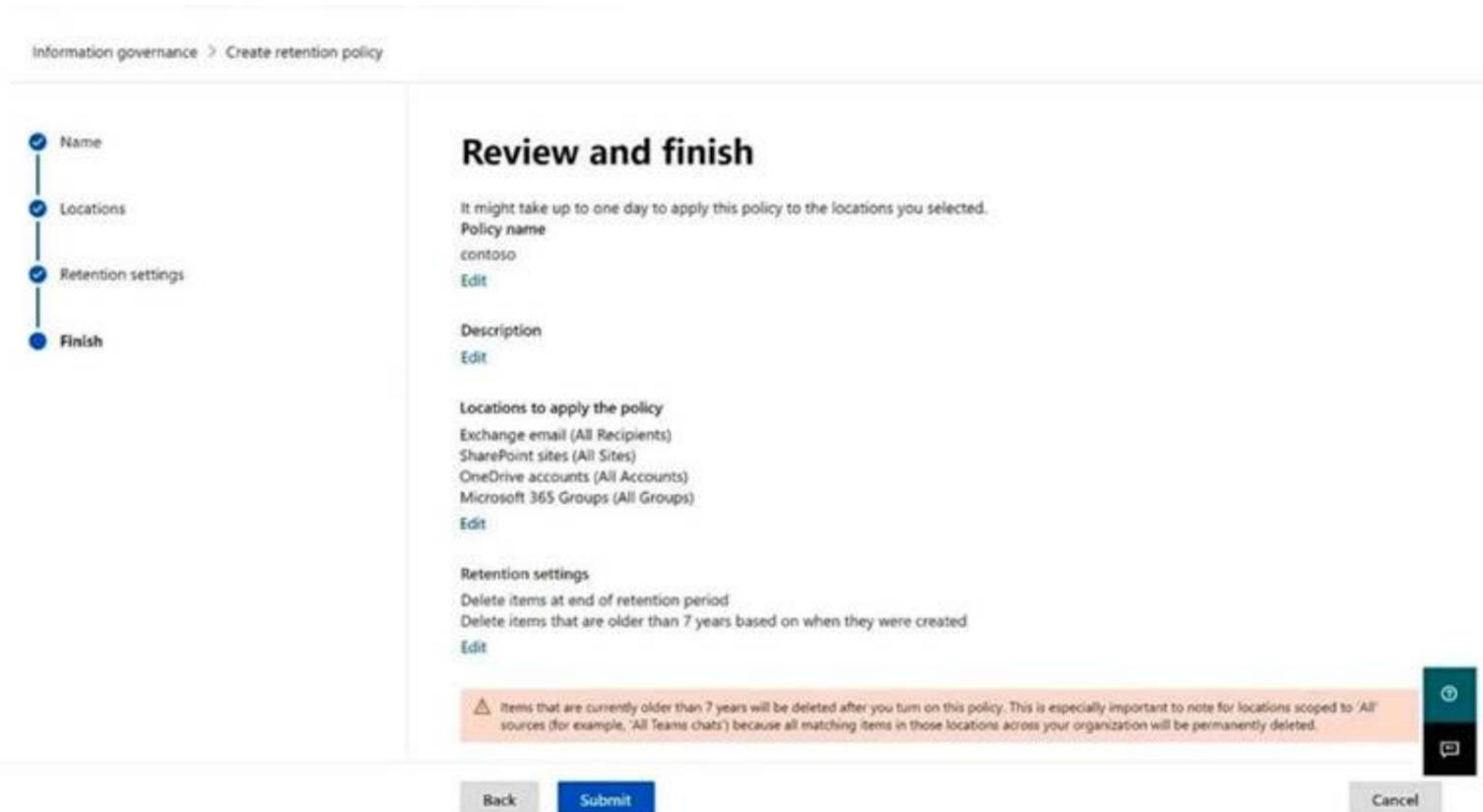
**NEW QUESTION 374**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.



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

**Answer Area**

Microsoft SharePoint files that are affected by the policy will be [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [answer choice].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Deleted seven years after they were created. From the exhibit:

The retention policy applies to SharePoint sites.

Delete items that are older than 7 years based on when they were created.

Box 2: data will retained for a minimum of seven years

The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.

Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5

years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.

**NEW QUESTION 379**

- (Topic 6)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

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

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

Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 380**

- (Topic 6)

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

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

Users in other departments must not be restricted.

What should you do?

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

**Answer: D**

**Explanation:**

Use the Microsoft 365 Defender portal to create Safe Links policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/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 381**

HOTSPOT - (Topic 6)

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

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

**NEW QUESTION 386**

- (Topic 6)

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

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

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

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

Answer: C

Explanation:

Reference:

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

**NEW QUESTION 390**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

## Microsoft Secure Score

Overview Improvement actions History Metrics & trends

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

↓ 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 391

- (Topic 6)

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

## Domains

+ Add domain Buy domain Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> Sub1.contoso221018.onmicrosoft.com (D...	⚠ Possible service issues	
<input type="checkbox"/> contoso.com	ⓘ Incomplete setup	
<input type="checkbox"/> contoso221018.onmicrosoft.com	✅ Healthy	
<input type="checkbox"/> Sub2.contoso221018.onmicrosoft.com	ⓘ Incomplete setup	

Which domain name suffixes can you use when you create users?

- A. only Sub1.contoso221018.onmicrosoft.com
- B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
- C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
- D. all the domains in the subscription

**Answer:** B

### NEW QUESTION 392

HOTSPOT - (Topic 6)

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

table.

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

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

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

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

NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, table Description automatically generated with medium confidence

**NEW QUESTION 395**

- (Topic 6)

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

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

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

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

**Answer:** C

**NEW QUESTION 400**

HOTSPOT - (Topic 6)

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

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

**Device limit restrictions**

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

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

Users may register their devices with Azure AD ⓘ

All  None

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

Require Multi-Factor Auth to join devices ⓘ

Yes  No

Maximum number of devices per user ⓘ

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 403

.....

## **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](#)**