

Exam Questions MS-102

Microsoft 365 Administrator Exam

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



NEW QUESTION 1

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

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

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

Answer Area

Teams daily active users:

| | |
|--------------------------|------------------------|
| <input type="checkbox"/> | Microsoft Secure Score |
| <input type="checkbox"/> | Adoption Score |
| <input type="checkbox"/> | Service health |
| <input type="checkbox"/> | Usage reports |

Recent Microsoft service issues:

| | |
|--------------------------|------------------------|
| <input type="checkbox"/> | Microsoft Secure Score |
| <input type="checkbox"/> | Adoption Score |
| <input type="checkbox"/> | Service health |
| <input type="checkbox"/> | Usage reports |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

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

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

Box 2: Service Health

Recent Microsoft service issues

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

NEW QUESTION 2

- (Topic 6)

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

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

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

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

Answer: D

Explanation:

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

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

Reference:

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

NEW QUESTION 3

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer: D

NEW QUESTION 4

- (Topic 6)

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

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

Answer: D

Explanation:

Reference:

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

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

NEW QUESTION 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.

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

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

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

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

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

- A. yes
- B. No

Answer: A

NEW QUESTION 6

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

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

NOTE: Each correct selection is worth one point.

Answer Area

| | |
|--------------|---|
| Portal: | <div><div>The Microsoft 365 admin center</div><div>The Microsoft 365 admin center</div></div> |
| Group types: | <div><div>The Microsoft 365 Defender portal</div><div>The Microsoft Entra admin center</div><div>The Microsoft Purview compliance portal</div></div> |
| Group types: | <div><div>Security only</div><div>Microsoft 365 only</div><div>Security only</div><div>Security and mail-enabled security only</div><div>Microsoft 365 and distribution only</div><div>Microsoft 365, mail-enabled security, and distribution only</div><div>Security, Microsoft 365, mail-enabled security, and distribution</div></div> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal:

The Microsoft 365 admin center
The Microsoft 365 admin center
The Microsoft 365 Defender portal
The Microsoft Entra admin center
The Microsoft Purview compliance portal

Group types:

Security only
Microsoft 365 only
Security only
Security and mail-enabled security only
Microsoft 365 and distribution only
Microsoft 365, mail-enabled security, and distribution only
Security, Microsoft 365, mail-enabled security, and distribution

NEW QUESTION 7

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 8

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 *:

Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

Added user, Deleted user, Reset user password, Changed user password, Changed user license, ... (7) ▾

Users:

Admin1 ✕

Duration *:

☒ 90 Days

☐ 6 Months

☐ 1 Year

Priority *:

100

Save

Cancel

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 9

- (Topic 6)

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

| Name | Type |
|--------|-----------------------|
| Group1 | Distribution |
| Group2 | Mail-enabled security |
| Group3 | Security |

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

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

Answer: A

Explanation:

Reference:

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

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

NEW QUESTION 10

- (Topic 6)

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

SharePoint Content_Export

Restart report

Download report

Delete

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

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

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

Close

Feedback

What will be excluded from the export?

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

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 10

- (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 12

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.

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

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

Answer: D

NEW QUESTION 16

- (Topic 6)
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must
Meet the following requirements.
Be serviced for a minimum of 24 months.
Support Microsoft Application Virtualization (App-V) Which version should you identify?

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

Answer: D

Explanation:

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

NEW QUESTION 19

- (Topic 6)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

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

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

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

Answer: D

NEW QUESTION 23

- (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 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 26

HOTSPOT - (Topic 6)
HOTSPOT
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

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

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

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

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

? Users or workload identities assignments: All users

? Cloud apps or actions assignment: App1

? Conditions: Include all trusted locations

? Grant access: Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

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

Box 2: Yes.

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

Box 3: No.

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

NEW QUESTION 28

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

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

Assignment

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

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

Answer Area

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

will lose the role after eight hours
 can reactivate the role every eight hours
 can reactivate the role every 15 days
 will lose the role after 15 days

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

for up to eight hours
 for up to three months
 for up to 15 days
 until the requests are revoked manually

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 33

HOTSPOT - (Topic 6)
 You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these

| Sensitive info type | Match accuracy |
|---------------------|----------------|
| | min max |
| Credit Card Number | 85 100 |

Retention labels

1 year

Add

+ Add group

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.

DLP1 cannot be applied to [answer choice].

Exchange email
SharePoint sites
OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

both a credit card number and the 1 year label applied
either a credit card number or the 1 year label applied
between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

NEW QUESTION 34

- (Topic 6)

Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription. You plan to implement a directory synchronization solution that will use password hash synchronization. From the Microsoft 365 admin center, you successfully verify the contoso.com domain name. You need to prepare the environment for the planned directory synchronization solution. What should you do first?

- A. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
- B. From the Microsoft 365 admin center verify the Contos
- C. Local domain name.
- D. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
- E. From Active Directory Users and Computers, modify the UPN suffix for all users.

Answer: A

NEW QUESTION 39

DRAG DROP - (Topic 6)

Your company has a Microsoft 365 E5 tenant. Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes. You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources. What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

Solution

Personal devices:

Solution

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy

NEW QUESTION 44

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 subscription. Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area



A. Mastered

B. Not Mastered

Answer: A

Explanation:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.



NEW QUESTION 46

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



i 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 48

HOTSPOT - (Topic 6)

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

| Name | Type | Member of |
|---------|--------|-----------|
| User1 | User | Group1 |
| Device1 | Device | Group2 |

User1 is the owner of Device1.

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 53

- (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 54

- (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.

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 55

- (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 60

- (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 64

HOTSPOT - (Topic 6)

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

| Name | Group | MFA Status |
|-------|----------------|------------|
| User1 | Group1 | Enabled |
| User2 | Group1, Group2 | Enforced |

You have the named locations shown in the following table.

| Named location | IP range |
|----------------|----------------|
| Montreal | 133.107.0.0/16 |
| Toronto | 193.77.10.0/24 |

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

- Users or workload identities: o Include: Group1
o Exclude: Group2
 - Cloud apps or actions: Include all cloud apps
 - Conditions: o Include: Any location o Exclude: Montreal
 - Access control: Grant access, Require multi-factor authentication User1 is on the multi-factor authentication (MFA) blocked users list.
- 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 Microsoft Office 365 from a device that has an IP address of 133.107.10.20. | <input type="radio"/> | <input type="radio"/> |
| User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15. | <input type="radio"/> | <input type="radio"/> |
| User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20. | <input checked="" type="radio"/> | <input type="radio"/> |
| User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15. | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 65

- (Topic 6)

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Health agent was installed on all the servers. You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.

You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.
- B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
- C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic
- D. From Windows PowerShell, run the Register-AzureADConnectHealthsyncAgent cmdlet.
- E. From Server1, reinstall the Azure AD Connect Health agent

Answer: DE

NEW QUESTION 69

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to meet the following requirements:

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

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 74

HOTSPOT - (Topic 6)

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

| Name | Member of | Role |
|-------|-----------|----------------------|
| User1 | Group1 | User Administrator |
| User2 | Group1 | None |
| User3 | Group2 | None |
| User4 | None | Global Administrator |

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR. Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

| | |
|--|--|
| Users that can use SSPR: | <div> <div>User1, User2, and User4 only</div> <div>User1 and User2 only</div> <div>User1, User2, and User3 only</div> <div>User1, User2, and User4 only</div> <div>User1, User2, User3, and User4</div> </div> |
| Users that must answer security questions to reset their password: | <div> <div>User1 and User2 only</div> <div>User1 only</div> <div>User2 only</div> <div>User1 and User2 only</div> <div>User1, User2, and User3 only</div> <div>User1, User2, and User4 only</div> <div>User1, User2, User3, and User4</div> </div> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| | |
|--|--|
| Users that can use SSPR: | <div> <div>User1, User2, and User4 only</div> <div>User1 and User2 only</div> <div>User1, User2, and User3 only</div> <div>User1, User2, and User4 only</div> <div>User1, User2, User3, and User4</div> </div> |
| Users that must answer security questions to reset their password: | <div> <div>User1 and User2 only</div> <div>User1 only</div> <div>User2 only</div> <div>User1 and User2 only</div> <div>User1, User2, and User3 only</div> <div>User1, User2, and User4 only</div> <div>User1, User2, User3, and User4</div> </div> |

NEW QUESTION 79

HOTSPOT - (Topic 6)

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

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

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

NOTE: Each correct selection is worth one point.

| | |
|-------------------|--|
| In Azure: | <div> <div></div> <div>Add and configure the Diagnostics settings for the Azure Activity Log.</div> <div>Add and configure an Azure Log Analytics workspace.</div> <div>Add an Azure Storage account and Azure Cognitive Search</div> <div>Add an Azure Storage account and a file share.</div> </div> |
| On the computers: | <div> <div></div> <div>Create an event subscription.</div> <div>Modify the membership of the Event Log Readers group.</div> <div>Enroll in Microsoft Endpoint Manager.</div> <div>Install the Microsoft Monitoring Agent.</div> </div> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

On the computers:

- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.












HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

Answer Area

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 86

- (Topic 6)

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

Updates

System controls restart during updates.   0%

| Name | Type | Version | Automatic Restart | Delayed Update | Options |
|--------|--------|----------|--|--|------------------------------|
| LOM DC | Driver | 1.17.034 |  on |  on | View details |

[View all updates](#)

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

- A. 20 hours
B. 12 hours

- C. 7 hours
- D. 48 hours

Answer: B

NEW QUESTION 87

- (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 90

HOTSPOT - (Topic 6)
HOTSPOT

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 91

HOTSPOT - (Topic 6)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

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

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
? Can be added to Compliance1 as recipients of noncompliance notifications
? Can be assigned to Compliance1

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

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

NEW QUESTION 94

- (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 97

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

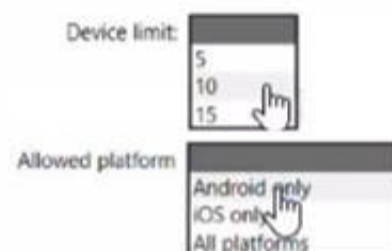
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)
 The device type restriction are configured as shown in the following table.

| 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 99

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

- From the Microsoft Entra admin center, configure on-premises integration password writeback.
- From the Microsoft Entra admin center, configure the authentication methods for SSPR.
- From the Microsoft Entra admin center, configure the registration settings for SSPR.
- Select Group writeback in Microsoft Entra Connect.
- Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2:

Step 3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- From the Microsoft Entra admin center, configure on-premises integration password writeback.
- From the Microsoft Entra admin center, configure the authentication methods for SSPR.
- From the Microsoft Entra admin center, configure the registration settings for SSPR.
- Select Group writeback in Microsoft Entra Connect.
- Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

NEW QUESTION 100

HOTSPOT - (Topic 6)

From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.

You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

| | | | |
|--|---------------------|--|--------|
| <div> <div>Set-RetentionCompliancePolicy</div> <div> Set-ComplianceTag Set-HoldCompliancePolicy Set-RetentionCompliancePolicy Set-RetentionPolicy Set-RetentionPolicyTag </div> </div> | -Identity "Policy1" | <div> <div>-RestrictiveRetention</div> <div> -enabled -Force -RestrictiveRetention -RetentionPolicyTagLinks -SystemTag </div> </div> | \$true |
|--|---------------------|--|--------|

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| | | | |
|--|---------------------|--|--------|
| <div> <div>Set-RetentionCompliancePolicy</div> <div> Set-ComplianceTag Set-HoldCompliancePolicy Set-RetentionCompliancePolicy Set-RetentionPolicy Set-RetentionPolicyTag </div> </div> | -Identity "Policy1" | <div> <div>-RestrictiveRetention</div> <div> -enabled -Force -RestrictiveRetention -RetentionPolicyTagLinks -SystemTag </div> </div> | \$true |
|--|---------------------|--|--------|

NEW QUESTION 103

- (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 104

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

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

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the

Security administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 107

HOTSPOT - (Topic 6)

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

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

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

| Name | Operating system |
|-----------|---------------------|
| Computer1 | Windows 10 |
| Computer2 | Windows Server 2016 |

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

Answer Area

Computer1:

Computer2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1:

Computer2:

NEW QUESTION 110

- (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 112

HOTSPOT - (Topic 6)

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

| Name | Role |
|--------|---------------------------|
| Admin1 | Global Administrator |
| Admin2 | Security Administrator |
| Admin3 | Security Operator |
| Admin4 | Security Reader |
| Admin5 | Application Administrator |

You are implementing Microsoft Defender for Endpoint.

You need to enable role-based access control (RBAC) to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and which users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users that can enable RBAC:

Admin1 and Admin2 only

Admin1 only

Admin1 and Admin2 only

Admin1, Admin2, and Admin5 only

Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

Admin3, Admin4, and Admin5 only

Admin5 only

Admin3 and Admin4 only

Admin4 and Admin5 only

Admin3, Admin4, and Admin5 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can enable RBAC:

Admin1 and Admin2 only

Admin1 only

Admin1 and Admin2 only

Admin1, Admin2, and Admin5 only

Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

Admin3, Admin4, and Admin5 only

Admin5 only

Admin3 and Admin4 only

Admin4 and Admin5 only

Admin3, Admin4, and Admin5 only

NEW QUESTION 114

- (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 Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

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 116

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 121

- (Topic 6)

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

| Name | Platform |
|---------|------------|
| Device1 | Windows 10 |
| Device2 | Android |
| Device3 | macOS |
| Device4 | iOS |

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

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

Answer: B

Explanation:

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

NEW QUESTION 125

HOTSPOT - (Topic 6)

HOTSPOT

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

Custom smart lockout

Lockout threshold ⓘ

15 ✓

Lockout duration in seconds ⓘ

600 ✓

Custom banned passwords

Enforce custom list ⓘ

Yes No

Custom banned password list ⓘ

3hundred
Eleven
Falcon
Project
Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes No

Mode ⓘ

Enforced Audit

User1 attempts to update their password to the following passwords:

? F@lcon

? Project22

? T4il\$pin45dg4

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

NOTE: Each correct selection is worth one point.

Answer Area

[Answer choice] will be accepted as a password.

▼

Only T4il\$pin45dg4

Only F@lcon and T4il\$pin45dg4

Only Project22 and T4il\$pin45dg4

F@lcon, Project22, and T4il\$pin45dg4

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

▼

will be locked out

will trigger a user risk

can attempt to sign in again immediately

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Only T4il\$pin45dg4

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

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

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

? Sign in to the Entra portal.

? Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.

? Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

? The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

? Set the Lockout duration in seconds, to the length in seconds of each lockout.

? The default is 60 seconds (one minute).

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

NEW QUESTION 129

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription.

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

An Exchange Online administrator recently created a role named Role1 from a computer on the network.

You need to identify the name of the administrator by using an audit log search.

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

NOTE: Each correct selection is worth one point.

Activities to search for:

| | |
|---------------------------------|---|
| | ▼ |
| Exchange mailbox activities | |
| Site administration activities | |
| Show results for all activities | |
| Role administration activities | |

Field to filter by:

| | |
|------------|---|
| | ▼ |
| Item | |
| User | |
| Detail | |
| IP address | |

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Activities to search for:

| | |
|---------------------------------|---|
| | ▼ |
| Exchange mailbox activities | |
| Site administration activities | |
| Show results for all activities | |
| Role administration activities | |

Field to filter by:

| | |
|------------|---|
| | ▼ |
| Item | |
| User | |
| Detail | |
| IP address | |

NEW QUESTION 131

- (Topic 6)

You have a Microsoft 365 subscription.

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

| Name | Role |
|-------|-------------------------------|
| User1 | Security Administrator |
| User2 | Global Administrator |
| User3 | Service Support Administrator |

You configure Tenant properties as shown in the following exhibit.

Technical contact

User1@contoso.com



Global privacy contact



Privacy statement URL

http://contoso.com/privacy



Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. Used only
- B. User2 only
- C. User3 only
- D. Used and User2 only
- E. User2 and User3 only

Answer: B

Explanation:

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

NEW QUESTION 136

- (Topic 6)

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.

Policy1

Edit policy

Delete policy

Status

On

Description

Add a description

Severity

Medium

Edit

Category

Information governance

Conditions

Activity is FileModified

Aggregation

Aggregated

Threshold

5 activities

Edit

Window

60 minutes

Scope

All users

Email recipients

User1@M365x082103.onmicrosoft.com

Daily notification limit

25

Edit

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours. How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25

Answer: D

NEW QUESTION 137

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 142

- (Topic 6)

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

What should you create in Microsoft Endpoint Manager?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 144

- (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 145

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. | |
| 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-igmpdomain -DomainId contoso.com. | Add a custom domain name. |
| Modify the email address of User1. | Verify the custom domain. |
| Add contoso.com as a SAN for an X.509 certificate. | Modify the username of User1. |
| Add a custom domain name. | |
| Verify the custom domain. | |
| Modify the username of User1. | |

NEW QUESTION 146

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.docx | 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.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Review your settings

Template name

Custom policy

Edit

Policy name

Policy1

Edit

Description

Edit

Applies to content in these locations

SharePoint sites

Edit

Policy settings

If the content contains these types of sensitive info: IP Address then notify people with a policy tip and email message.
If there are at least 2 instances of the same type of sensitive info, block access to the content.

Edit

Turn policy on after it's created?

Yes

Edit

How many files will be visible to user1 and User2 after Policy1 is applied to answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Passing Certification Exams Made Easy

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

Answer Area

Use 1:

1

2

3

4

5

Use 2:

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Use 1:

1

2

3

4

5

Use 2:

1

2

3

4

5

NEW QUESTION 151

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

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☐

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☐
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☐

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

☐

No

☒

User2@contoso.com will receive an incident notification email for the alert at 08:07.

☒
☐

User1@contoso.com will receive an incident notification email for the alert at 08:20.

☐
☒

NEW QUESTION 154

- (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 158

- (Topic 6)

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

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

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

To which users can User1 send documents that contain PII?

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

Answer: B

NEW QUESTION 160

HOTSPOT - (Topic 6)

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

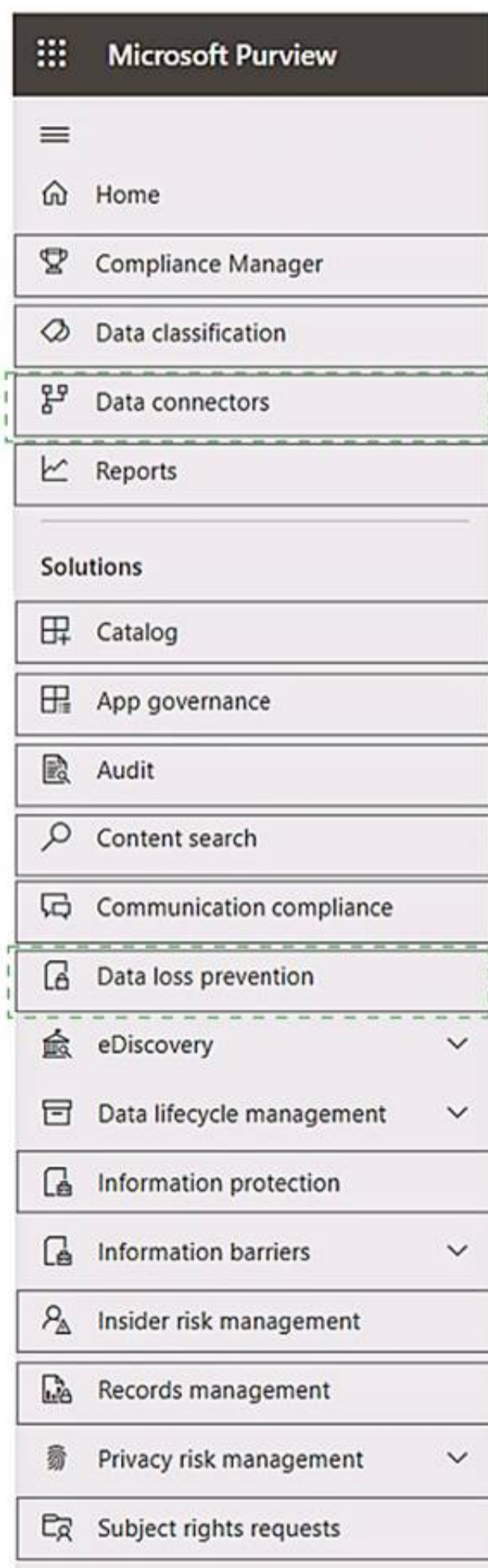


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 161

- (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 163

- (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 165

- (Topic 6)

Your company has a Microsoft E5 tenant.

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

What should you use?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 169

- (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 174

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

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

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

| User | Date |
|-------|----------|
| User1 | August 5 |
| User2 | August 7 |

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

User1:

▼

August 6

August 17

August 19

September 3

September 5

User2:

▼

August 8

August 17

August 19

August 21

September 7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: August 19

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

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

Box 2: August 21

NEW QUESTION 179

- (Topic 6)

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

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

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

Another administrator configures the domain to synchronize to Azure AD.

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

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

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

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

NEW QUESTION 180

- (Topic 6)

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

Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

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

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

Answer: ABE

Explanation:

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

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

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

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

(A) In your on-premises environment

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

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

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

* 4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

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

Incorrect:

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

Reference:

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

NEW QUESTION 182

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription. You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. 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:

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

- * 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
- * 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
- * 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
- * 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
- * 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

NEW QUESTION 185

- (Topic 6)

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. What permission should you assign to User1?

- A. the Information Protection administrator role from the Azure Active Directory admin center.
- B. the eDiscovery Manager role from the Microsoft 365 compliance center.
- C. the Compliance Management role from the Exchange admin center.
- D. the User management administrator role from the Microsoft 365 admin center.

Answer: B

NEW QUESTION 186

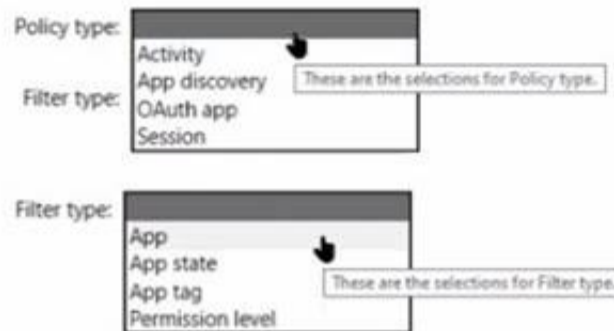
HOTSPOT - (Topic 6)

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

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

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

Answer Area

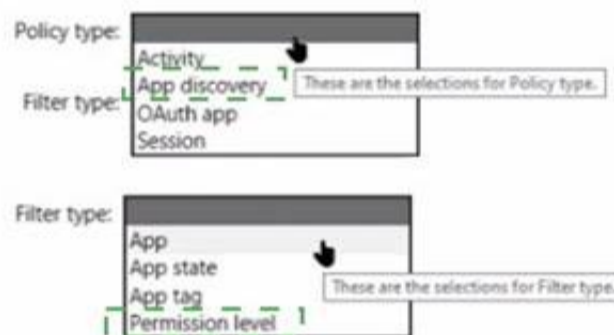


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 189

- (Topic 6)

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

Company policy requires that the devices have the following configurations:

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

You need to configure the devices to meet the requirements.

What should you use?

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

Answer: B

Explanation:

Reference:

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

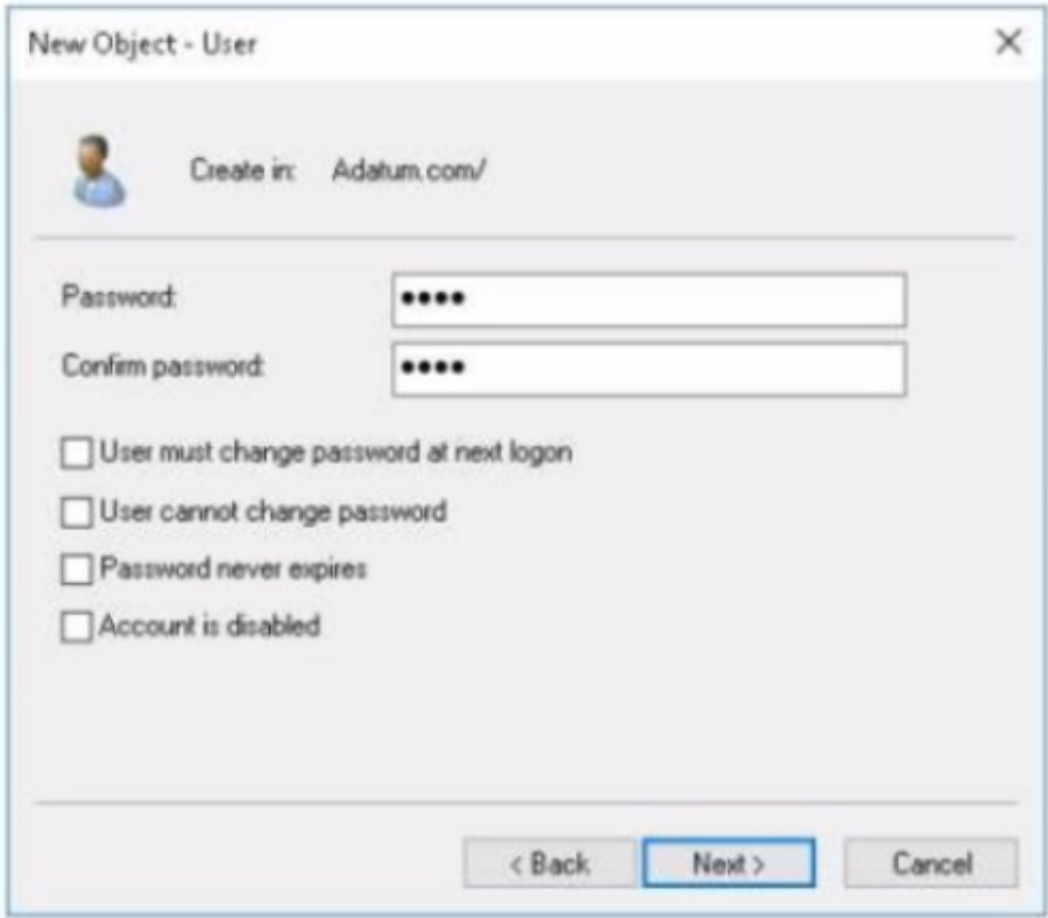
NEW QUESTION 192

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 195

HOTSPOT - (Topic 6)

You work at a company named Contoso, Ltd.
Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.
Contoso purchases a company named Fabrikam, Inc.
Contoso plans to add the following domains to the Microsoft 365 subscription:

- fabrikam.com
- east.fabrikam.com
- west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Domains:

3

1

2

3

Enterpriseregistration DNS records:

3

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Domains:

3

1

2

3

Enterpriseregistration DNS records:

3

1

2

3

NEW QUESTION 198

- (Topic 6)
 You have a Microsoft 365 subscription.
 You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.
 Which type of group should you use to assign the Reports Reader role and to access App1?

- A. a Microsoft 365 group that has assigned membership
- B. a Microsoft 365 group that has dynamic user membership
- C. a security group that has assigned membership
- D. a security group that has dynamic user membership

Answer: C

Explanation:

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can't be members of security groups. Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.

Reference:
<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps> <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?> <https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>

NEW QUESTION 200

HOTSPOT - (Topic 6)
 You have device compliance policies shown in the following table.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 205

- (Topic 6)

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

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

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

| Name | UPN suffix |
|-------|--------------|
| User1 | Contoso.com |
| User2 | Fabrikam.com |

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

A. Yes
B. No

Answer: B

Explanation:

This is not a permissions issue. The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 209

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 ⓘ

5

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

| 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 214

- (Topic 6)

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

| Name | Platform | Azure Active Directory (Azure AD) |
|---------|------------|-----------------------------------|
| Device1 | Windows 10 | Joined |
| Device2 | Windows 10 | Registered |
| Device3 | Windows 10 | Not joined or registered |
| Device4 | Android | Registered |

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION 217

HOTSPOT - (Topic 6)

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

| Name | Platform | BitLocker Drive Encryption (BitLocker) | Member of |
|---------|------------|--|----------------|
| Device1 | Windows 10 | Disabled | Group1, Group2 |
| Device2 | Windows 10 | Disabled | Group2, Group3 |
| Device3 | Windows 10 | Disabled | Group3 |

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

| Name | Require BitLocker | Mark noncompliant after (days) | Assigned |
|---------|-------------------|--------------------------------|----------|
| Policy1 | Require | 5 | No |
| Policy2 | Require | 10 | Yes |
| Policy3 | Not configured | 15 | Yes |

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

| Name | Assigned to |
|---------|-------------|
| Policy2 | Group2 |
| Policy3 | Group3 |

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 222

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

| Policy | Default Shared Folder Location | Default Office Theme |
|---------------------|---|----------------------|
| All users | https://sharepoint.contoso.com/addins_all_users | Colorful |
| Office Users Policy | https://sharepoint.contoso.com/addins_office_users | White |
| Sales Team Policy | https://sharepoint.contoso.com/addins_sales_team_users_ | Dark Gray |

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users
https://sharepoint.contoso.com/addins_office_users
https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

Colorful
Dark Gray
White

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users
https://sharepoint.contoso.com/addins_office_users
https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

Colorful
Dark Gray
White

NEW QUESTION 225

DRAG DROP - (Topic 6)
DRAG DROP

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

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

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

Actions

Answer Area

Authorize Server1.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run GenConnectorConfig.ps1 on Server1.

Run GenConnectorConfig.ps1 on Server2.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 228

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

File type to use:

| |
|------|
| CSV |
| JSON |
| PST |
| XML |

Required properties for each user:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

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

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

? Select Add multiple users.

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

? Etc.

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

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

Box 2: User Name and Display Name

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

NEW QUESTION 230

HOTSPOT - (Topic 5)

You need to ensure that Admin4 can use SSPR.

Which tool should you use. and which action should you perform? To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action:

Tool:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Action:

Tool:

NEW QUESTION 235

- (Topic 3)

You create the planned DLP policies.

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 236

- (Topic 3)

You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

- A. Replace
- B. Enable redirect
- C. Block
- D. Dynamic Delivery

Answer: D

Explanation:

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md>

NEW QUESTION 239

- (Topic 3)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 243

HOTSPOT - (Topic 3)

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

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

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

NOTE: Each correct selection is worth one point.

Supported devices:

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

Number of required profiles:

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Supported devices:

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

Number of required profiles:

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

NEW QUESTION 246

HOTSPOT - (Topic 2)

You need to meet the technical requirement for log analysis.

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

NOTE: Each correct selection is worth one point.

Minimum number of data sources:

| |
|---|
| ▼ |
| 1 |
| 3 |
| 6 |

Minimum number of log collectors:

| |
|---|
| ▼ |
| 1 |
| 3 |
| 6 |

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 248

HOTSPOT - (Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

| |
|------------------------|
| ▼ |
| Audit log |
| Data governance events |
| DLP policy matches |
| eDiscovery |

Filter by:

| |
|------------|
| ▼ |
| Activity |
| Detail |
| Item |
| User agent |

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 253

- (Topic 2)

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

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

Answer: B

Explanation:

References:

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

NEW QUESTION 257

- (Topic 1)

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

- A. User2
 B. User3

- C. User4
- D. User5

Answer: C

Explanation:

References:

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

NEW QUESTION 261

- (Topic 1)

On which server should you use the Defender for identity sensor?

- A. Server1
- B. Server2
- C. Server3
- D. Server4
- E. Servers5

Answer: A

Explanation:

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

NEW QUESTION 265

- (Topic 2)

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

Answer: C

Explanation:

References:

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

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

NEW QUESTION 269

- (Topic 1)

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

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

Answer: C

Explanation:

References:

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

NEW QUESTION 272

- (Topic 1)

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices. What is the minimum of dedicated support technicians required?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 276

- (Topic 6)

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

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

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

What should you configure?

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

Answer: D

NEW QUESTION 281

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that.

You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.

Which feature should you use, and how many days will the data be retained? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Feature:

Number of days the data will be retained:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature:

Number of days the data will be retained:

NEW QUESTION 284

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

Compliance settings [Edit](#)

Microsoft Defender ATP

Require the device to be at or under the machine risk score:

Low

Device Health

Rooted devices

Require the device to be at or under the Device Threat Level

Block

System Security

Require a password to unlock mobile devices

Required password type

Encryption of data storage on device.

Block apps from unknown sources

Require

Device default

Require

Block

Actions for noncompliance [Edit](#)

Action

Schedule

Mark device noncompliant

Immediately

Retire the noncompliant device

Immediately

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.

When a device reports a medium threat level, the device will

▼

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

▼

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When a device reports a medium threat level, the device will

▼

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

▼

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

NEW QUESTION 289

HOTSPOT - (Topic 6)

HOTSPOT

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

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

All the groups are deleted.

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

NOTE: Each correct selection is worth one point.

Groups that can be restored:

▼

Group3 only

Group1 and Group2 only

Group2 and Group4 only

Group1, Group2, and Group3 only

Group1, Group2, Group3, and Group4

Retention period:

▼

24 hours

7 days

14 days

30 days

90 days

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Group3 only

Box 2: 30 days

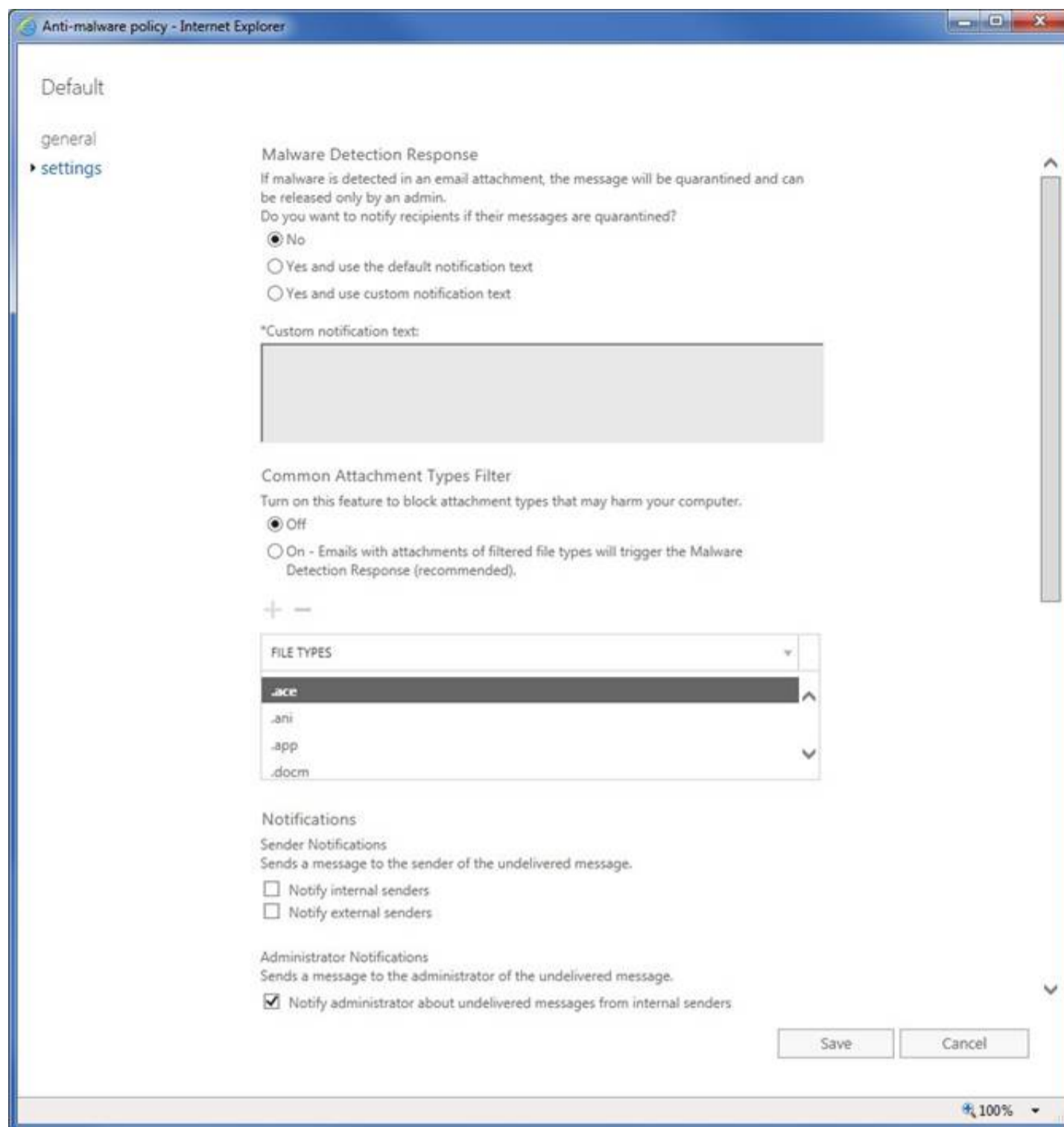
If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

NEW QUESTION 294

- (Topic 6)

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

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



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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 297

- (Topic 6)

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

Groups | All groups ...
Contoso Ltd. - Azure Active Directory

New group Download groups Refresh Manage view Delete Got feedback?

Search Search mode Contains Add filter

4 groups found

| | Name | Group type | Security enabled | Role assignments allowed |
|--------------------------|--------|---------------|------------------|--------------------------|
| <input type="checkbox"/> | Group1 | Microsoft 365 | No | No |
| <input type="checkbox"/> | Group2 | Microsoft 365 | Yes | No |
| <input type="checkbox"/> | Group3 | Security | Yes | No |
| <input type="checkbox"/> | Group4 | Security | Yes | Yes |

To which groups can you assign Microsoft 365 E5 licenses?

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

Answer: C

NEW QUESTION 301

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario.

Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

| Name | UPN suffix |
|-------|--------------|
| User1 | Contoso.com |
| User2 | Fabrikam.com |

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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

NEW QUESTION 305

HOTSPOT - (Topic 6)

HOTSPOT

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

| Name | Members |
|------|--------------|
| AU1 | User1, User2 |
| AU2 | User3 |

You have the following users:

? A user named User1 that is assigned the Password Administrator for AU1 and AU2.

? A user named User2 that is assigned the User Administrator for AU1.

? A user named User3 that is assigned the User Administrator for the tenant.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1 can reset the password of User3.

☒
☐

User2 can update the display name of User1.

☐
☐

User1 can reset the password of User2.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Administrator.

Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

| Role that password can be reset | Password Admin | Helpdesk Admin | Auth Admin | User Admin | Privileged Auth Admin | Global Admin |
|---------------------------------|--------------------------|----------------|------------|------------|-----------------------|--------------|
| User Admin | <input type="checkbox"/> | | | ✓ | ✓ | ✓ |
| Usage Summary Reports Reader | | ✓ | ✓ | ✓ | ✓ | ✓ |

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Administrator.

Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins.

NEW QUESTION 308

- (Topic 6)

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

You need to ensure that users can select a department when they enroll their device in Intune.

What should you create?

- A. scope tags

- B. device configuration profiles
- C. device categories
- D. device compliance policies

Answer: C

Explanation:

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

NEW QUESTION 310

HOTSPOT - (Topic 6)

HOTSPOT

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

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

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -eq "Guest"
Dynamic membership rules for groups in Azure Active Directory
Supported expression operators
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

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

Box 2: -contains "Support" Incorrect:

- * -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.

NEW QUESTION 313

HOTSPOT - (Topic 6)

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

- ? Prevent users from enrolling personal devices.
 - ? Ensure that users can enroll a maximum of 10 devices.
- What should you use for each requirement? To answer, select the appropriate options in the answer area.
- NOTE: Each correct selection is worth one point.

Prevent users from enrolling
personal devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

Ensure that users can enroll a
maximum of 10 devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Prevent users from enrolling
personal devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

Ensure that users can enroll a
maximum of 10 devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

NEW QUESTION 316

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

| Name | Retention period | During the retention period |
|------------|------------------|-----------------------------------|
| Retention1 | 5 years | Retain items even if users delete |
| Retention2 | 5 years | Mark items as a record |
| Retention3 | 5 years | Mark items as a regulatory record |

Site1 contains the files shown in the following table.

| Name | Label |
|-------|------------|
| File1 | None |
| File2 | Retention1 |
| File3 | Retention2 |
| File4 | Retention3 |

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Rename:

File1 only
 File1 and File2 only
File1, File2, and File3 only
 File1, File2, File3, and File4

Delete:

File1 only
File1 and File2 only
 File1, File2, and File3 only
 File1, File2, File3, and File4

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Rename:

File1 only
 File1 and File2 only
File1, File2, and File3 only
 File1, File2, File3, and File4

Delete:

File1 only
File1 and File2 only
 File1, File2, and File3 only
 File1, File2, File3, and File4

NEW QUESTION 319

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Alert
 Threat
 Compliance

Role:

Quarantine
 Security Administrator
 Organization Configuration
 Communication Compliance Admin

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Alert
 Threat
 Compliance

Role:

Quarantine
 Security Administrator
 Organization Configuration
 Communication Compliance Admin

NEW QUESTION 322

- (Topic 6)

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

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

What should you do first?

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

Answer: D

NEW QUESTION 323

HOTSPOT - (Topic 6)

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

From the Sign-ins blade of the Microsoft Entra admin center for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 can view the sign-ins for the following users:

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

User2 can view the sign-ins for the following users:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 can view the sign-ins for the following users:

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

User2 can view the sign-ins for the following users:

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

NEW QUESTION 324

- (Topic 6)

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.

You purchase 100 Microsoft 365 Business Voice add-on licenses.

You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.

What should you do?

- A. From the Microsoft 365 admin center, modify the settings of the Voice group.
- B. From the Licenses page of the Microsoft 365 admin center, assign the licenses.
- C. From the Microsoft Entra admin center, modify the settings of the Voice group.

Answer: C

NEW QUESTION 329

- (Topic 6)

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

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.

Which role should you assign to User1?

- A. View-Only Audit Logs in the Security & Compliance admin center
- B. View-Only Audit Logs in the Exchange admin center
- C. Security reader in the Azure Active Directory admin center
- D. Security Reader in the Security & Compliance admin center

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide>

NEW QUESTION 334

- (Topic 6)

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

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

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

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

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

Answer: C

NEW QUESTION 339

- (Topic 6)

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

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

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

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

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 344

- (Topic 6)

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

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

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

Answer: C

NEW QUESTION 345

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records.

You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

- A. Configure custom detection rules.
- B. Create an Exact Data Match (EDM) schema.
- C. Run the Sec-RegulatoryComplianceUI cmdlet.
- D. Run the Sec-LabelPolicy cmdlet.

Answer: C

Explanation:

Reference:

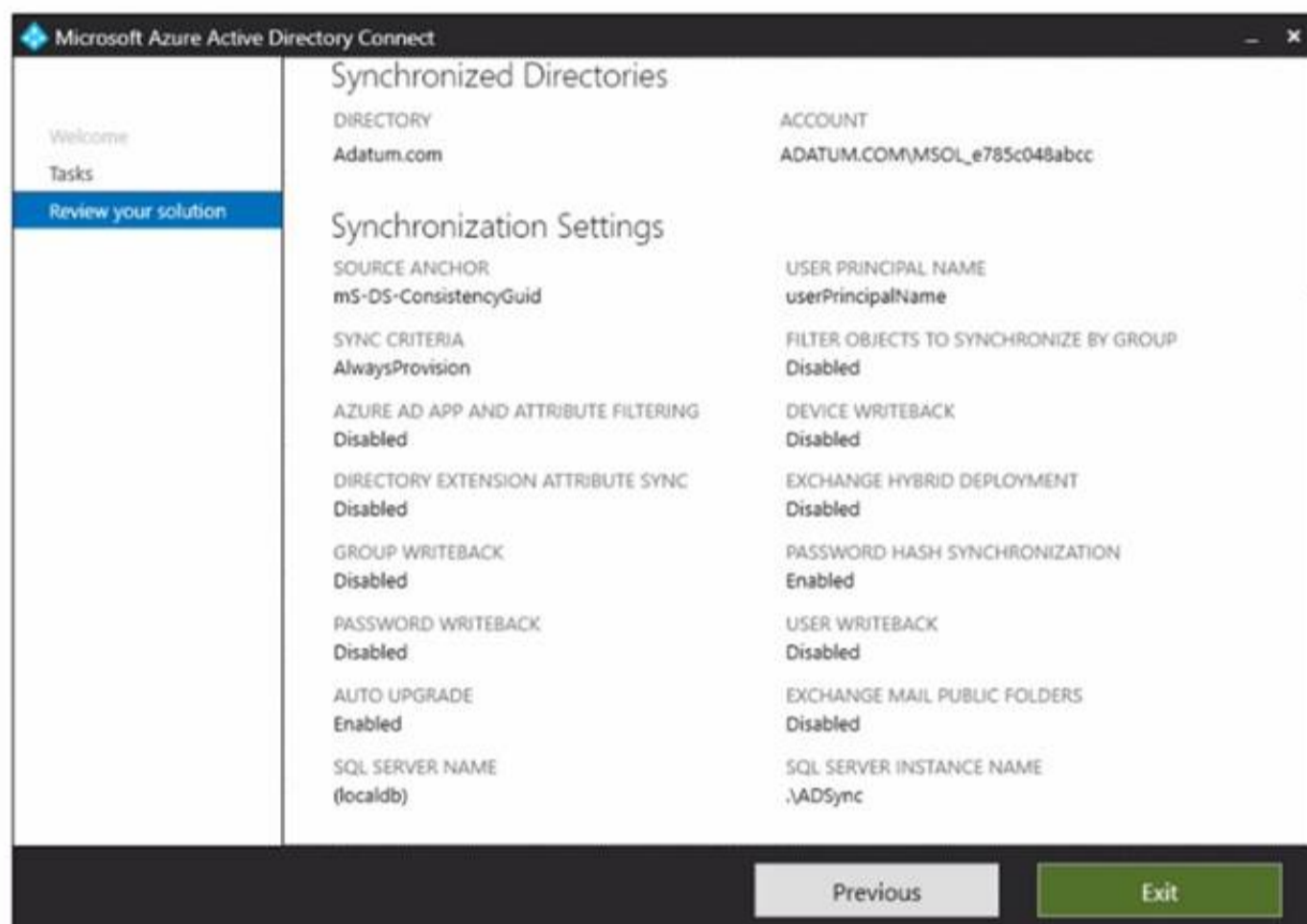
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

NEW QUESTION 347

HOTSPOT - (Topic 6)

Your company has a hybrid deployment of Microsoft 365. An on-premises user named User1 is synced to Azure AD.

Azure AD Connect is configured 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

User1 [answer choice].

If the password for User1 is changed in Active Directory, [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 [answer choice].

If the password for User1 is changed in Active Directory, [answer choice].

NEW QUESTION 352

- (Topic 6)

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

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

- A. yes
- B. No

Answer: A

NEW QUESTION 355

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. 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 |
|--|-----------------------|-----------------------|
| You can add Admin1 as a member of AU1. | <input type="radio"/> | <input type="radio"/> |
| You can add User1 as a member of AU2. | <input type="radio"/> | <input type="radio"/> |
| You can assign Admin2 the User administrator role for AU1. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| You can add Admin1 as a member of AU1. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can add User1 as a member of AU2. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can assign Admin2 the User administrator role for AU1. | <input type="radio"/> | <input checked="" type="radio"/> |

NEW QUESTION 358

- (Topic 6)

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

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the domain functional level to Windows Server 2019. You copy the

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

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 362

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

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

Money Back Guarantee

MS-102 Practice Exam Features:

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