



Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1

HOTSPOT - (Topic 6)

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

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

The tenant contains the devices shown in the following table.

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

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

Statements

Yes No

Device1 is marked as compliant.

☐
☐

Device2 is marked as compliant.

☐
☐

Device3 is marked as compliant.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

Yes No

Device1 is marked as compliant.

☒
☐

Device2 is marked as compliant.

☒
☐

Device3 is marked as compliant.

☐
☒

NEW QUESTION 2

- (Topic 6)

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

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

The solution must use the principle of least privilege.

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 3

DRAG DROP - (Topic 6)
DRAG DROP

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

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

The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1:

Role

Group2:

Role

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Billing admin manage service request Purchase new services Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin User admin
Assign the User admin role to users who need to do the following for all users:

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

NEW QUESTION 4

HOTSPOT - (Topic 6)
HOTSPOT

You have a Microsoft 365 subscription.
You need to review metrics for the following: The daily active users in Microsoft Teams Recent Microsoft service issues
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Guaranteed success with Our exam guides

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

Answer Area

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

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

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

Box 2: Service Health

Recent Microsoft service issues

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

NEW QUESTION 5

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

- A. Yes
 B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 6

DRAG DROP - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to automatically label the documents on Site1 that contain credit card numbers. 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

Create a sensitivity label.

Create an auto-labeling policy.

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Publish the label.

Create a retention label.

Wait eight hours, and then turn on the policy.

Answer Area

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

Create a sensitivity label.

Create an auto-labeling policy.

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

Publish the label.

Create a retention label.

Wait eight hours, and then turn on the policy.

Answer Area

Create a sensitivity label.

Publish the label.

Create an auto-labeling policy.

NEW QUESTION 7

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

To identify when users have compromised credentials, configure:

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password

Require multi-factor authentication

Require password change

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: A user risk policy

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

User risk-based Conditional Access policy

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

Block access

Allow access but require a secure password change.

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

Box 2: Require password change

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

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

NEW QUESTION 8

- (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 admin role.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 9

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

? Report on shared documents that contain PII.

What should you create?

A. an alert policy

B. a data loss prevention (DLP) policy

C. a retention policy

D. a Microsoft Cloud App Security policy

Answer: B

Explanation:

Reference:

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

NEW QUESTION 10

- (Topic 6)

You have a Microsoft 365 subscription.

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

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 10

- (Topic 6)

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

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only

B. Mailbox1, Account1, and Site1 only

C. Account1 and Site1 only

D. Mailbox1, Account1, Site1, and Channel1

E. Account1, Site1, and Channel1 only

Answer: E

Explanation:

Reference:

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

NEW QUESTION 14

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

Answer: A

Explanation:

Use Conditional Access policies

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

Reference:

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

NEW QUESTION 18

- (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 22

- (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 25

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:

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

- 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 29

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 31

- (Topic 6)
 You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy. You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps. Which policy type should you configure?

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

Answer: A

Explanation:

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

NEW QUESTION 33

- (Topic 6)
 Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10. You purchase a Microsoft 365 subscription. You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO). You need to ensure that users can use Seamless SSO from the Windows 10 computers. What should you do?

- A. Join the computers to Azure AD.
- B. Create a conditional access policy in Azure AD.
- C. Modify the Intranet zone settings by using Group Policy.
- D. Deploy an Azure AD Connect staging server.

Answer: A

NEW QUESTION 37

- (Topic 6)
 You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint. You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint. You need to identify which user can view security incidents from the Microsoft 365 Defender portal. Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Answer: A

NEW QUESTION 39

- (Topic 6)

You have a Microsoft 365 subscription.

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

What should you do?

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

Answer: A

NEW QUESTION 42

- (Topic 6)

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

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

- A. Group1 only
- B. Group2 only
- C. Site1 only
- D. Group1 and Group2 only
- E. Group1, Group2, and Site1

Answer: E

Explanation:

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.

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.

When you configure a label policy, you can:

Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

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

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

NEW QUESTION 44

- (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 47

- (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 52

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 55

- (Topic 6)

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

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

Which properties of the alerts can you modify?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 60

- (Topic 6)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

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

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

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

- A. Yes
- B. No

Answer: A

NEW QUESTION 64

HOTSPOT - (Topic 6)

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

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy

Name *

Policy1

Description

Record Types

AzureActiveDirectory

Activities

Added user

Users:

Show results for all users

Duration *

☐ 90 Days

☒ 6 Months

☐ 1 Year

Priority *

100

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

Answer Area

Admin1:

6 months

30 days

90 days

6 months

1 year

Admin2:

90 days

30 days

90 days

6 months

1 year

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Admin1:

6 months

30 days

90 days

6 months

1 year

Admin2:

90 days

30 days

90 days

6 months

1 year

NEW QUESTION 69

- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

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

Answer: A

NEW QUESTION 74

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Role
User1	Global admin
User2	None
User3	None

You provision the private store in Microsoft Store for Business.

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

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

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

NOTE: Each correct selection is worth one point.

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

NEW QUESTION 77

- (Topic 6)

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

- A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
- B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
- C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
- D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Answer: A

Explanation:

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

NEW QUESTION 80

HOTSPOT - (Topic 6)

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

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy to create in Microsoft Endpoint Manager:

▼

An app configuration policy

An app protection policy

A conditional access policy

A device compliance policy

Minimum number of required policies:

▼

1

2

3

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy to create in Microsoft Endpoint Manager:

▼

An app configuration policy

An app protection policy

A conditional access policy

A device compliance policy

Minimum number of required policies:

▼

1

2

3

5

NEW QUESTION 82

- (Topic 6)

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

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

The devices are managed by using Microsoft Intune.

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

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

Answer: A

NEW QUESTION 83

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

MFA method:

Call to phone

Email message

Security questions

Text message to phone

Notification to Microsoft Authenticator app

Number of days:

7

14

30

60

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Notification to Microsoft Authenticator app

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

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

Box 2: 14

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

NEW QUESTION 88

- (Topic 6)

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a trainable classifier
- B. a sensitive info type
- C. an insider risk policy
- D. an adaptive policy scope
- E. a data loss prevention (DLP) policy

Answer: AE

Explanation:

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition Communication compliance

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.

Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

NEW QUESTION 92

- (Topic 6)

You have a Microsoft 365 E5 tenant.

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

- A. From Policy in the Azure portal, select Compliance, and then assign a pokey
- B. From Compliance Manager, create an assessment
- C. From the Microsoft J6i compliance center, create an audit retention policy.
- D. From the Microsoft 365 admin center enable the Productivity Score.

Answer: B

NEW QUESTION 93

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

The device limit restrictions in Endpoint manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

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

Answer Area	Statements	Yes	No
	User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
	User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
	User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:
 Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 96

- (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 departments 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 101

- (Topic 6)

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

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

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

You plan to implement directory synchronization.

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

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

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

- A. Yes
 B. No

Answer: A

NEW QUESTION 106

- (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 107

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.

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:

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 111

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

Message center

New service request

Product feedback

Service health

Answer Area

To report issues regarding a Microsoft 365 service:

New service request

To request help on how to add a new user to the tenant:

Message center

NEW QUESTION 113

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:

Add and configure the Diagnostics settings for the Azure Activity Log.

Add and configure an Azure Log Analytics workspace.

Add an Azure Storage account and Azure Cognitive Search

Add an Azure Storage account and a file share.

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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In Azure:

Add and configure the Diagnostics settings for the Azure Activity Log.

Add and configure an Azure Log Analytics workspace.

Add an Azure Storage account and Azure Cognitive Search

Add an Azure Storage account and a file share.

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.

NEW QUESTION 117

- (Topic 6)

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

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

Where can you store data from the LinkedIn connector?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 120

- (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 123

- (Topic 6)

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

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

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

? To all users, deploy an Office 365 E3 license without the Power Automate license option.

? To all users, deploy an Enterprise Mobility + Security E5 license.

? To the users in the research department only, deploy a Power BI Pro license.

? To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

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

Answer: C

Explanation:

One for all users, one for the research department, and one for the marketing department.

Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

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

NEW QUESTION 125

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

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

? Opening files in Microsoft SharePoint that contain malicious content

? Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Opening files in SharePoint that contain malicious content:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

NEW QUESTION 128

- (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 130

HOTSPOT - (Topic 6)

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

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

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

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

You apply DLP1 to Site1.

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

NOTE: Each correct selection is worth one point.

Answer Area

File1:

Tip2 only

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 and Tip2 only

Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

File1:

Tip2 only

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 and Tip2 only

Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

NEW QUESTION 133

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 136

- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1 You create a retention label named Retention1 that is published to all locations. You need to ensure that User1 can label email messages by using Retention1 as soon as possible.
Which cmdlet should you run in Microsoft Exchange Online PowerShell?

- A. Start-MpScan
- B. Start-Process
- C. Start-ManagedFolderAsslstant
- D. Start-AppBackgroundTask

Answer: C

NEW QUESTION 140

- (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 141

HOTSPOT - (Topic 6)

You have a Microsoft 365 Enterprise E5 subscription.

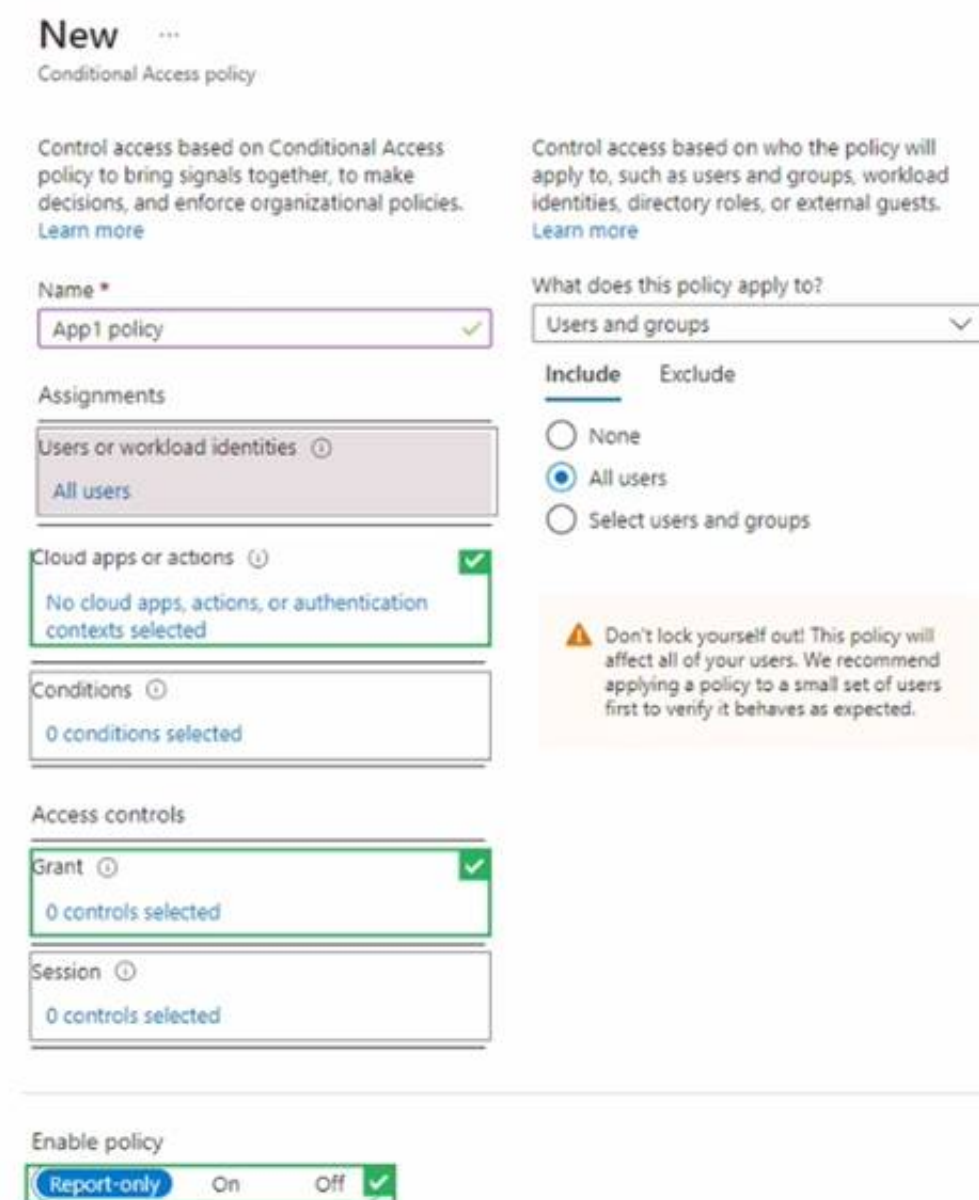
You add a cloud-based app named App1 to the Azure AD enterprise applications list.

You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? 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

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *

Assignments

Users or workload identities

All users

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☒ All users

☐ Select users and groups

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Report-only On Off

Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

NEW QUESTION 142

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.

All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).

You plan to create a user named Admin1 that will perform following tasks:

- View BitLocker recovery keys.
- Configure the usage location for the users in contoso.com.

You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.

NOTE: Each correct selection is worth one point

Answer Area**Devices**

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

NEW QUESTION 145

- (Topic 6)

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

- Windows 10
- Android
- OS

On which devices can you configure the Endpoint DLP policies?

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

Answer: D

Explanation:

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

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

NEW QUESTION 148

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

? Scope type: Directory

? Selected members: Group1

? Assignment type: Active

? Assignment starts: Mar 15, 2023

? Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

? Scope type: Directory

? Selected members: Group2

? Assignment type: Eligible

? Assignment starts: Jun 15, 2023

? Assignment ends: Oct 15, 2023

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

NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

Admin1 is member of Group1.

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

July 15, 2023 is with the assignment period.

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

Box 2: No

Admin2 is member of Group2.

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

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

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

Box 3: Yes

Admin3 is member of Group1 and Group2.

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

May 1, 2023 is with the assignment period.

NEW QUESTION 149

HOTSPOT - (Topic 6)

HOTSPOT

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

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

Site1 contains the files shown in the following table.

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

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

Rule1 tip only

Rule2 tip only

Rule3 tip only

Rule1 tip and Rule2 tip only

Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

Rule1 tip only

Rule3 tip only

Rule4 tip only

Rule1 tip and Rule4 tip only

Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).
It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

NEW QUESTION 152

- (Topic 6)
You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling (preview)

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

+ Create a label Publish labels Refresh

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

Which labels can users apply to content?

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

Answer: C

NEW QUESTION 155

- (Topic 6)

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

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

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

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

Answer: B

NEW QUESTION 160

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

? Block a vulnerable app until the app is updated.

? Block an application executable based on a file hash.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Block a vulnerable app until the app is updated:

▼

An allow or block file

A file indicator

A remediation request

An update ring

Block an application executable based on a file hash:

▼

An allow or block file

A file indicator

A remediation request

An update ring

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

? Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

? Select a security recommendation to see a flyout with more information.

? Select Request remediation.

? Select whether you want to apply the remediation and mitigation to all device groups or only a few.

? Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

? Pick a Remediation due date and select Next.

? Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.

? Review the selections you made and Submit request. On the final page you can

choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

NEW QUESTION 162

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 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 168

- (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 172

HOTSPOT - (Topic 6)

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

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

NEW QUESTION 174

- (Topic 6)

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN



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

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

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 179

HOTSPOT - (Topic 6)

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

- ? Show app and profile configuration progress: Yes
- ? Allow users to collect logs about installation errors: Yes
- ? Only show page to devices provisioned by out-of-box experience (OOBE): No
- ? Assignments: Group2

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 181

- (Topic 6)

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

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

You have a computer that runs Windows 10.

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

Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

- A. Yes
 B. No

Answer: B

NEW QUESTION 186

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 188

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

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

Answer: C

Explanation:

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

Specific types of sensitive information.

Specific keywords that match a query you create.

Pattern matches for a trainable classifier.

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

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels) Teams chats

Teams private channel messages Yammer community messages Yammer user messages

Reference:

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

NEW QUESTION 191

- (Topic 6)

You have a Microsoft 365 tenant.

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

? Require complex passwords.

? Require the encryption of data storage devices.

? Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 194

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).

You need to create a detection exclusion in Azure ATP. Which tool should you use?

- A. the Security & Compliance admin center
- B. Microsoft Defender Security Center
- C. the Microsoft 365 admin center
- D. the Azure Advanced Threat Protection portal
- E. the Cloud App Security portal

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/defender-for-identity/what-is> <https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections>

NEW QUESTION 199

- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You need to access service health alerts from a mobile phone. What should you use?

- A. the Microsoft Authenticator app
- B. the Microsoft 365 Admin mobile app
- C. Intune Company Portal
- D. the Intune app

Answer: B

NEW QUESTION 202

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table. User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:

- Which administrators can unblock User1
- What to configure to allow User1 to send at least 2,000 emails per day without being blocked

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

Answer Area

Administrators:

Settings:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Administrators:

Settings:

NEW QUESTION 203

- (Topic 6)
You have a Microsoft 365 subscription. Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de- fghij. You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs. D18912E1457D5D1DDCBD40AB3BF70D5D What should you create to ensure that the DLP policy can detect the customer IDs?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 207

- (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 211

- (Topic 6)

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

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

You enable device clean-up rules

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

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

Answer: D

NEW QUESTION 215

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. End point analytics

- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

Answer: D

NEW QUESTION 219

HOTSPOT - (Topic 6)

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

Name	Membership type	Membership rule
Group1	Assigned	<i>Not applicable</i>
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

The subscription contains the users shown in the following table.

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	<i>None</i>
User3	R&D	Group1

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

- Assignments o Users

Include: Group1

Exclude: Group2. Group3 o Target resources

Cloud apps App1

Access controls Grant

Block access

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 App1.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to App1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to App1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can sign in to App1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to App1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in to App1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 221

- (Topic 6)

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

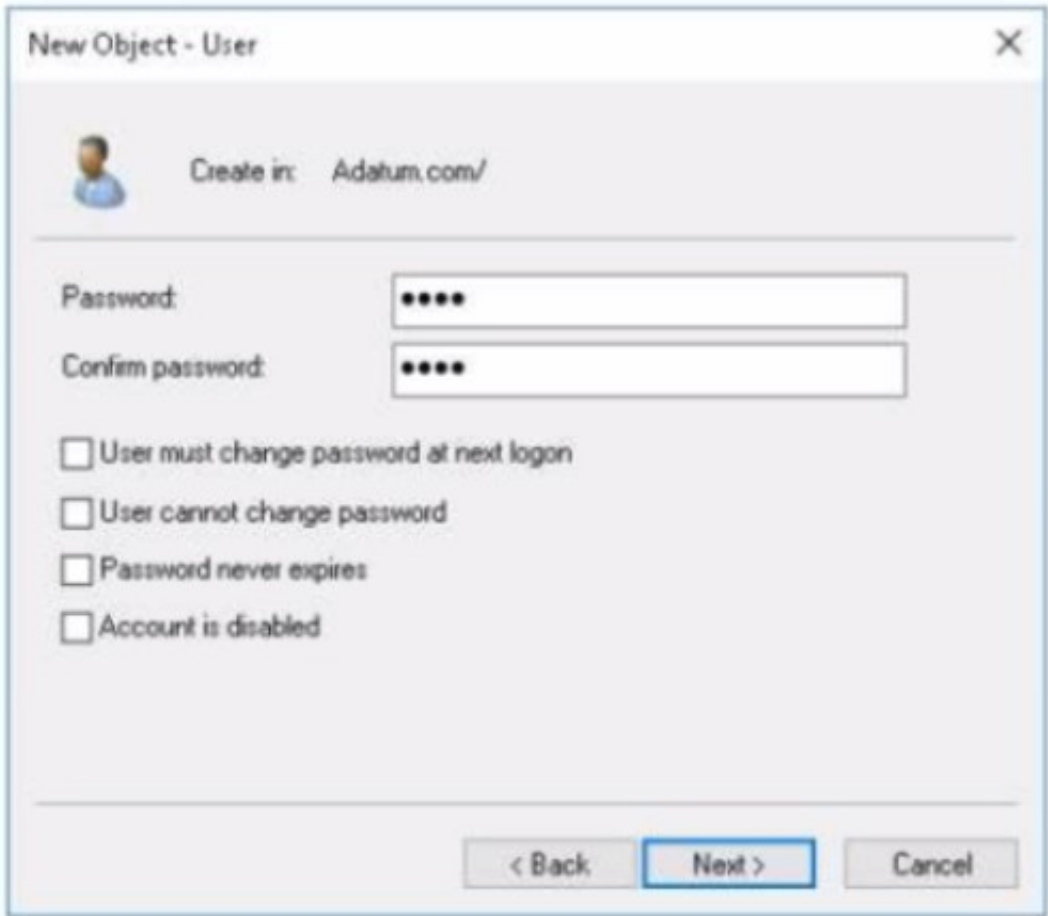
- A. the Information Protection administrator ide from the Azure Active Directory admin center.
- B. the eDiscovery Manager tote from the Microsoft 365 compliance center.
- C. the Compliance Management role from the Exchange admin center.
- D. the User management administrator role from the Microsoft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

Answer: B

NEW QUESTION 226

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 229

HOTSPOT - (Topic 6)

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

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

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

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

You perform the following actions:

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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<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:

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

NEW QUESTION 233

- (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 234

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 235

DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to review reports to identify the following:

- The storage usage of files stored in Microsoft Teams
- The number of active users per team

Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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

Report

The device usage report in Teams

The OneDrive usage report

The SharePoint site usage report

The Teams usage report in Teams

The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams:

Number of active users per Microsoft Team:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Report

The device usage report in Teams

The OneDrive usage report

The SharePoint site usage report

The Teams usage report in Teams

The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams:

The SharePoint site usage report

Number of active users per Microsoft Team:

The Teams usage report in Teams

NEW QUESTION 240

HOTSPOT - (Topic 6)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:

Device 1 only

Device 1 and Device 2 only

Device 1 and Device 3 only

Device 1 and Device 4 only

Device 1, Device 2, and Device 4 only

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

Endpoint security policies that must be configured:

A conditional access policy only

A device compliance policy only

A device configuration profile only

A device configuration profile and a conditional access policy only

Device configuration profile, device compliance policy, and conditional access policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

NEW QUESTION 243

- (Topic 6)

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

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

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

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

Answer: C

NEW QUESTION 245

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.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 249

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

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

You have the apps shown in the following table.

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

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 250

- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

- A. From the Cloud App Security admin center, select Users and accounts.
- B. From the Microsoft 365 security center, view the Threat tracker.
- C. From the Microsoft 365 admin center, view the Security & compliance report.
- D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

NEW QUESTION 251

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant.
You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

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

Auto-labeling policy

[Edit Policy](#)[Delete Policy](#)

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 254

DRAG DROP - (Topic 6)
DRAG DROP

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

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

You use Azure Information Protection.

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

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

Actions

Authorize Server1.

Install the Microsoft Rights Management connector on Server2.

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run GenConnectorConfig.ps1 on Server1.

Run GenConnectorConfig.ps1 on Server2.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	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 255

- (Topic 6)
You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

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

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

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

Answer: D

NEW QUESTION 257

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 260

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:

Enable password writeback.
Enable app registrations.
Enable password writeback.
Enable password hash synchronization.
Disable password hash synchronization.

Tool:

Azure AD Connect
Azure AD Connect
Synchronization Rules Editor
Microsoft Entra admin center

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Action:

Enable password writeback.
Enable app registrations.
Enable password writeback.
Enable password hash synchronization.
Disable password hash synchronization.

Tool:

Azure AD Connect
Azure AD Connect
Synchronization Rules Editor
Microsoft Entra admin center

NEW QUESTION 265

HOTSPOT - (Topic 5)
You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.
Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Users:

Admin1 and Admin3 only
Admin1 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and Admin4

Blade:

Service Health
Reports
Service Health
Message center

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users:

Admin1 and Admin3 only

Admin1 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and Admin4

Blade:

Service Health

Reports

Service Health

Message center

NEW QUESTION 270

- (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 271

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 274

- (Topic 3)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 278

- (Topic 2)

You need to meet the technical requirement for large-volume document retrieval. What should you create?

- A. a data loss prevention (DLP) policy from the Security & Compliance admin center
- B. an alert policy from the Security & Compliance admin center
- C. a file policy from Microsoft Cloud App Security
- D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts>

NEW QUESTION 283

- (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 284

HOTSPOT - (Topic 1)

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

NOTE: Each correct selection is worth one point.

Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date
References:
<https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>

NEW QUESTION 289

HOTSPOT - (Topic 1)
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

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

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 293

- (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 298

- (Topic 1)

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

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

Answer: C

NEW QUESTION 299

- (Topic 1)

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

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

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

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

You configure a pilot for co-management.

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

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

- A. Yes
- B. NO

Answer: A

Explanation:

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: <https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable>

NEW QUESTION 302

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

NOTE: Each correct selection is worth one point.

Answer Area

Sign-in risk policy:	<div><div>Leaked credentials</div><div>Atypical travel</div><div>Leaked credentials</div><div>Possible attempt to access Primary Refresh Token (PRT)</div></div>
User risk policy:	<div><div>Malicious IP address</div><div>Leaked credentials</div><div>Malicious IP address</div><div>Suspicious browser</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Sign-in risk policy:	<div><div>Leaked credentials</div><div>Atypical travel</div><div>Leaked credentials</div><div>Possible attempt to access Primary Refresh Token (PRT)</div></div>
User risk policy:	<div><div>Malicious IP address</div><div>Leaked credentials</div><div>Malicious IP address</div><div>Suspicious browser</div></div>

NEW QUESTION 305

- (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 307

- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. a sensitive info type
- C. a data loss prevention (DLP) policy
- D. a sensitivity label
- E. a retention label
- F. a retention label policy

Answer: CE

NEW QUESTION 310

DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune. You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices. Which four 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

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

>

<

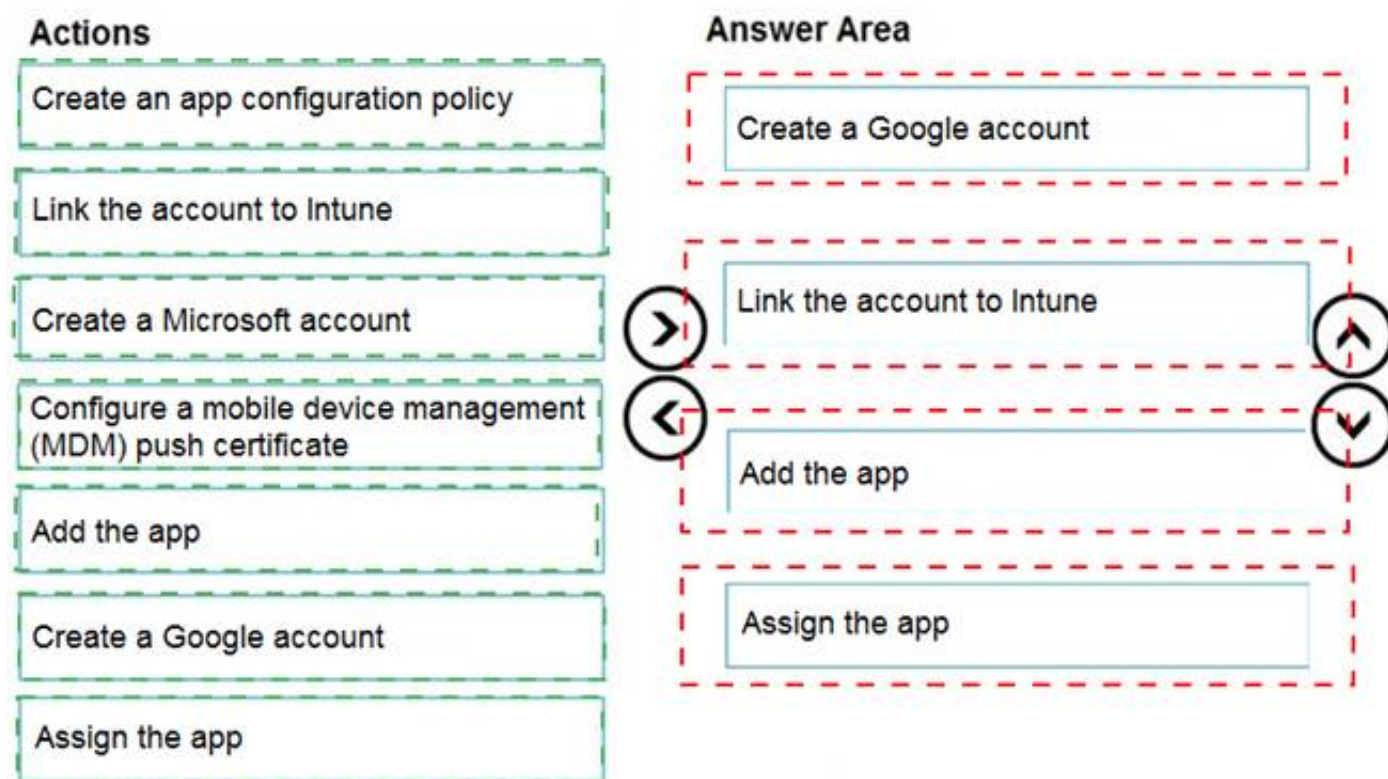
↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 312

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

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

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

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

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

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

Answer: B

Explanation:

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

One Policy.

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

One Policy.

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

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

One policy

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

Reference:

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

NEW QUESTION 316

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 319

- (Topic 6)
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?

- A. CSV
- B. XLSX
- C. JSON
- D. XML

Answer: B

Explanation:
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template>

NEW QUESTION 324

- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

- A. Yes
- B. No

Answer: A

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

NEW QUESTION 326

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

User1 can reset the password of User3.

Yes

☐

No

☐

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 329

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Your company's Microsoft Secure Score recommends the actions shown in the following exhibit.

Microsoft Secure Score

Overview

Recommended actions

History

Metrics & trends

↓

Export

Rank	Recommended action	Score impact	Points achieved	Status
<input type="checkbox"/> 1	Require multifactor authentication for administrative roles	+4.15%	0/10	<input type="radio"/> To address
<input type="checkbox"/> 2	Ensure all users can complete multifactor authentication	+3.73%	0/9	<input type="radio"/> To address
<input type="checkbox"/> 3	Create Safe Links policies for email messages	+3.73%	0/9	<input type="radio"/> To address
<input type="checkbox"/> 4	Enable policy to block legacy authentication	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/> 5	Turn on Safe Attachments in block mode	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/> 6	Ensure that intelligence for impersonation protection is enabled	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/> 7	Move messages that are detected as impersonated users by mailbox intelligence	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/> 8	Enable impersonated domain protection	+3.32%	0/8	<input type="radio"/> To address

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.
 How does the change affect the Secure Score?

- A. remains the same
- B. increases by 1 point
- C. increases by 9 points
- D. decreases by 1 point
- E. decreases by 9 points

Answer: A

NEW QUESTION 334

- (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 338

- (Topic 6)

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.

The domain contains 100 user accounts.
 The city attribute for all the users is set to the city where the user resides.
 You need to modify the value of the city attribute to the three-letter airport code of each city.
 What should you do?

- A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec- ADUser cmdlets.
- B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.
- C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace- MgUser cmdlets.
- D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

Answer: A

Explanation:

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on- premise Active Directory.
 You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.

Note:

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

- * 1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
- * 2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.

Other incorrect answer options you may see on the exam include the following:

- * 1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
- * 2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set- AzureADUser cmdlets.
- * 3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
- * 4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser>

NEW QUESTION 341

- (Topic 6)

You are reviewing alerts in the Microsoft 365 Defender portal. How long are the alerts retained in the portal?

- A. 30 days
- B. 60 days
- C. 3 months
- D. 6 months
- E. 12 months

Answer: C

Explanation:

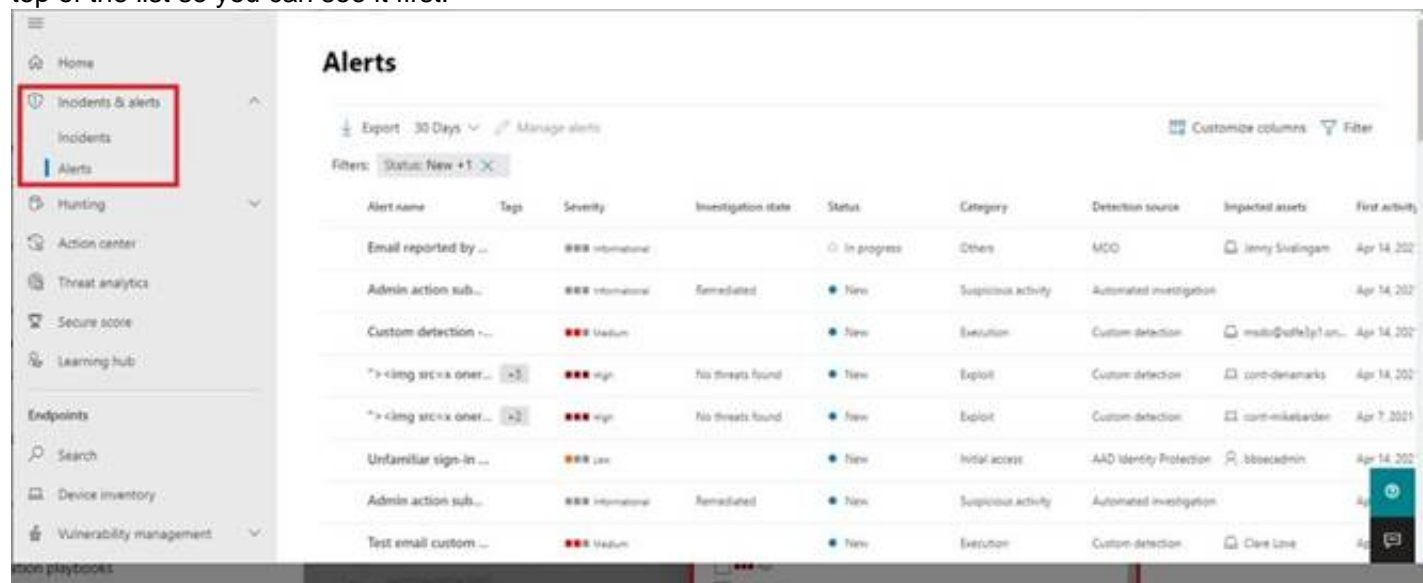
Data retention information for Microsoft Defender for Office 365

By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.

Defender for Office 365 Plan 1

- * Alert metadata details (Microsoft Defender for Office alerts) 90 days.

Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.



Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data- retention>

NEW QUESTION 346

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 351

- (Topic 6)

Your network contains an Active Directory forest named contoso.local. You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.

You need to prepare for the planned move to Microsoft 365.

What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.
- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

Answer: D

Explanation:

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on- premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization>

NEW QUESTION 354

HOTSPOT - (Topic 6)

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

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

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

Data Transfer

Backup org data to Android backup services ⓘ

AllowBlock

Send org data to other apps ⓘ

Policy managed apps

Select apps to exempt

Select

Save copies of org data ⓘ

AllowBlock

Allow user to save copies to selected services ⓘ

SharePoint

Transfer telecommunication data to ⓘ

Any dialer app

Dialer App Package ID

Dialer App Name

Receive data from other apps ⓘ

All Apps

Open data into Org documents ⓘ

AllowBlock

Allow users to open data from selected services ⓘ

3 selected

Restrict cut, copy, and paste between other apps ⓘ

Policy managed apps with paste in

Screen capture and Google Assistant ⓘ

AllowBlock

Approved keyboards ⓘ

RequireNot required

Select keyboards to approve

Select

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

Answer Area

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

Microsoft SharePoint Online

OneDrive

local storage

Microsoft SharePoint Online

Microsoft SharePoint Online and OneDrive

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

any app

any app

only managed apps

only unmanaged apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

Microsoft SharePoint Online

OneDrive

local storage

Microsoft SharePoint Online

Microsoft SharePoint Online and OneDrive

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

any app

any app

only managed apps

only unmanaged apps

NEW QUESTION 356

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 360

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.

You need to meet the following requirements:

- * View an assessment of the device configurations against the Center for Internet Security (CIS) v1.0.0 benchmark.
- Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.

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

Answer Area

To view the device configuration assessment:

Create a baseline assessment profile.

Add a connected application.

Create a baseline assessment profile.

Filter the Vulnerable devices report.

To protect C:\Folder1, enable:

Controlled folder access

Controlled folder access

Exploit protection

Removable storage protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To view the device configuration assessment:

Create a baseline assessment profile.

Add a connected application.

Create a baseline assessment profile.

Filter the Vulnerable devices report.

To protect C:\Folder1, enable:

Controlled folder access

Controlled folder access

Exploit protection

Removable storage protection

NEW QUESTION 364

- (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 367

- (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 369

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

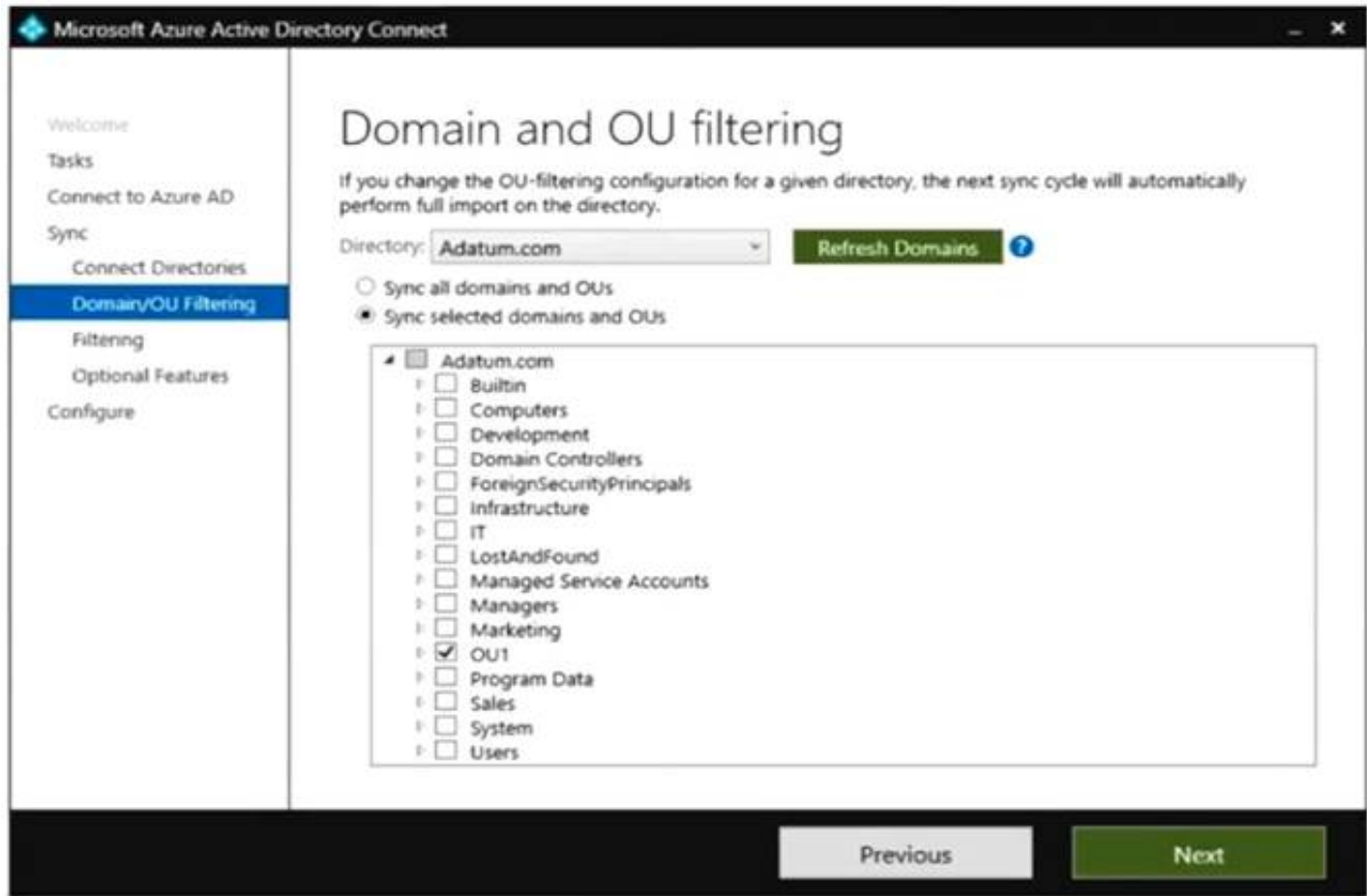
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



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



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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 372

- (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.

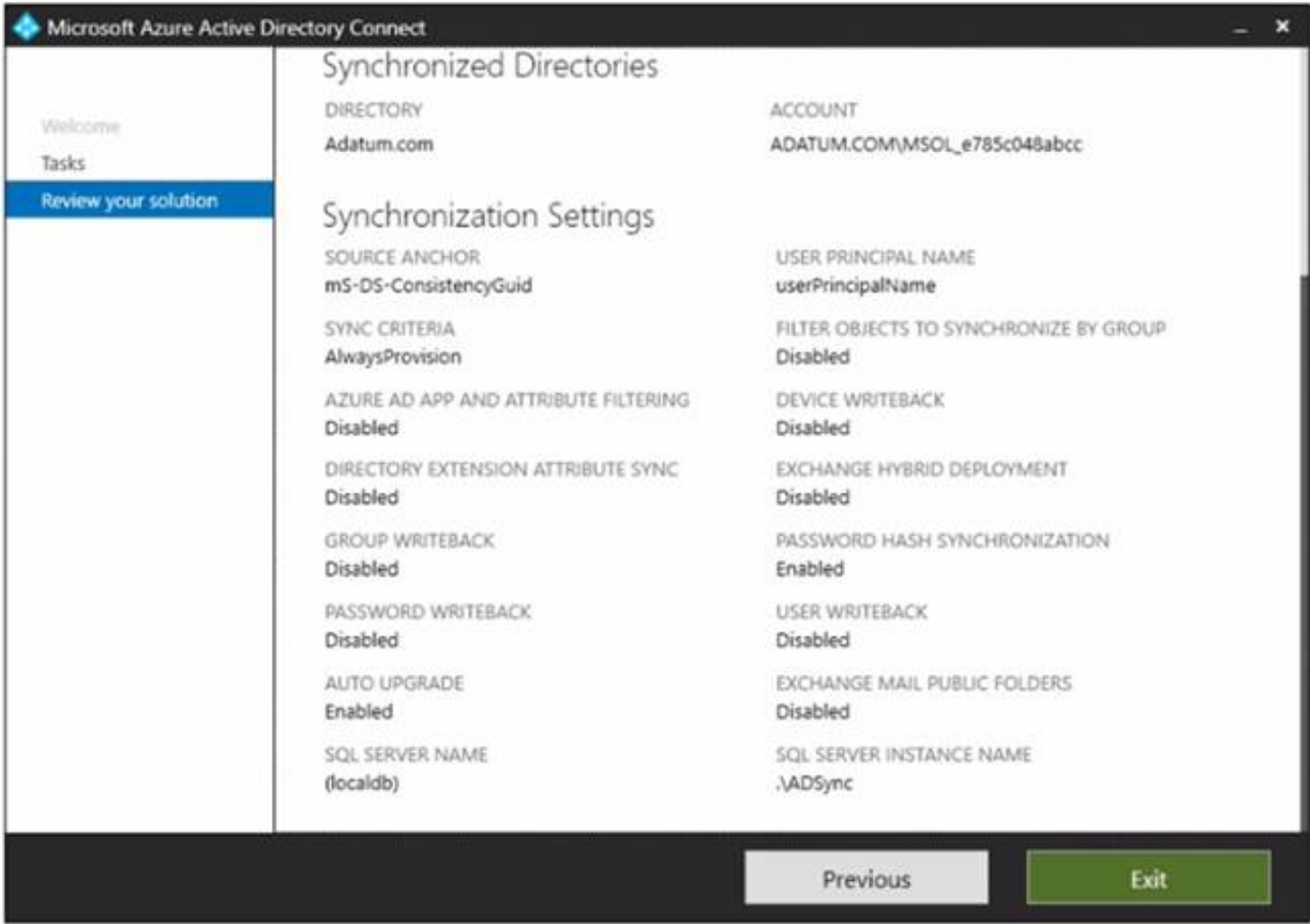
Answer: C

Explanation:

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

NEW QUESTION 376

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].

cannot change her password from any Microsoft portals

cannot change her password from any Microsoft portals

can change her password by using self-service password reset feature only

can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory,

[answer choice].

the password hash will be synchronized to Azure AD

the password hash will be synchronized to Azure AD

a new randomly generated password will be assigned to User1

the password hash in Azure AD will be unchanged

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 [answer choice].

cannot change her password from any Microsoft portals

cannot change her password from any Microsoft portals

can change her password by using self-service password reset feature only

can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory,

[answer choice].

the password hash will be synchronized to Azure AD

the password hash will be synchronized to Azure AD

a new randomly generated password will be assigned to User1

the password hash in Azure AD will be unchanged

NEW QUESTION 381

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

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