

Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam



NEW QUESTION 1

- (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 2

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install:

Server:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

NEW QUESTION 3

- (Topic 6)

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

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

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

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

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

? Administrative effort must be minimized.

What should you include in the recommendation?

A. device categories

B. scope tags

C. configuration profiles

D. conditional access policies

Answer: B

Explanation:

Reference:

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

NEW QUESTION 4

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

A. an attack surface reduction (ASR) policy

B. an app configuration policy

C. a device compliance policy

D. a device configuration profile

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

NEW QUESTION 5

- (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 6

- (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 7

- (Topic 6)

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 9

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 10

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

What should you use?

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

Answer: C

NEW QUESTION 10

- (Topic 6)

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

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

What should you do on the computer?

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

Answer: B

NEW QUESTION 11

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: CE

NEW QUESTION 15

- (Topic 6)

Your company has multiple offices.

You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.

You need to ensure that the local administrators can manage only the devices in their respective office.

What should you use?

- A. scope tags

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

Answer: A

Explanation:

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

NEW QUESTION 16

HOTSPOT - (Topic 6)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Reset the password of User4:

User1 and User3 only

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Reset the password of User4:

User1 and User3 only

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

NEW QUESTION 17

HOTSPOT - (Topic 6)

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.

Configure

Microsoft Intune

Save

Discard

Delete

MDM user scope ⓘ

None

Some

All

Groups

Select groups

Group1

MDM terms of use URL ⓘ

https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL ⓘ

https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL ⓘ

https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM User scope ⓘ

None

Some

All

Groups

Select groups

Group2

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ

https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL ⓘ

Restore default MAM URLs

You purchase a Windows 10 device named Device1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 20

- (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 Mailbox! as a SecOps mailbox.
- D. Place a litigation hold on Mailbox1.

Answer: D

NEW QUESTION 22

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 27

- (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 subscription.

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

Solution: From the Endpoint Management admin center, you create a device configuration profile.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 31

- (Topic 6)

Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.

You plan to implement a directory synchronization solution that will use password hash synchronization.

From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.

You need to prepare the environment for the planned directory synchronization solution. What should you do first?

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

Answer: A

NEW QUESTION 36

- (Topic 6)

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

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for

10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

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

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

Answer: B

Explanation:

Storage locations

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

* Machine information

- Stored in a Log Analytics workspace.

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

Reference:

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

NEW QUESTION 37

- (Topic 6)

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

What should you do next?

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

Answer: C

NEW QUESTION 40

- (Topic 6)

You have a Microsoft 365 subscription.

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

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

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

 Report an issue  Customize

Active issues

Issue title Affected service Issue type

> Microsoft service health (6)

Issues in your environment that require action (0)

Microsoft service health

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

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

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

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

Answer: B

Explanation:

Service Support admin

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

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

Incorrect:

* Message center reader

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

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

* Reports reader

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

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

Reference:

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

NEW QUESTION 45

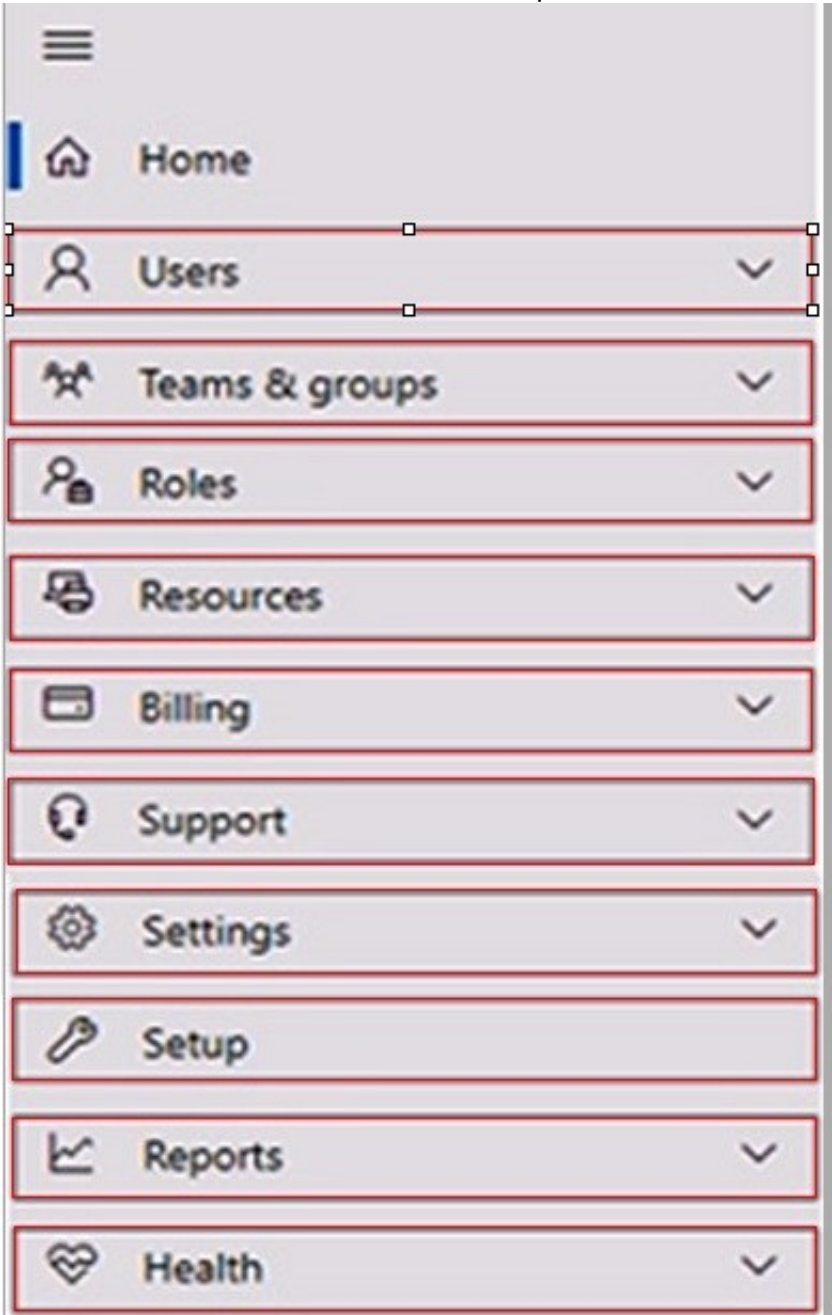
HOTSPOT - (Topic 6)

HOTSPOT

Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks:

View the Adoption Score of the company. Create a new service request to Microsoft.

Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score To enable Adoption Score:

? Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score

? Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

NEW QUESTION 50

- (Topic 6)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

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

Answer: B

NEW QUESTION 55

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	<i>None</i>
User3	<i>None</i>

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

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

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

Can add apps to the private store:

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 60

- (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 61

- (Topic 6)

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

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

Answer: C

Explanation:

View email security reports in the Microsoft 365 Defender portal

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

Reference:

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

NEW QUESTION 66

- (Topic 6)

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

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

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

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

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

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

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

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

- A. Yes
- B. No

Answer: B

NEW QUESTION 70

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:

<input type="checkbox"/>	Call to phone
<input type="checkbox"/>	Email message
<input type="checkbox"/>	Security questions
<input type="checkbox"/>	Text message to phone
<input type="checkbox"/>	Notification to Microsoft Authenticator app

Number of days:

<input type="checkbox"/>	7
<input type="checkbox"/>	14
<input type="checkbox"/>	30
<input type="checkbox"/>	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 71

- (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 76

HOTSPOT - (Topic 6)

HOTSPOT

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

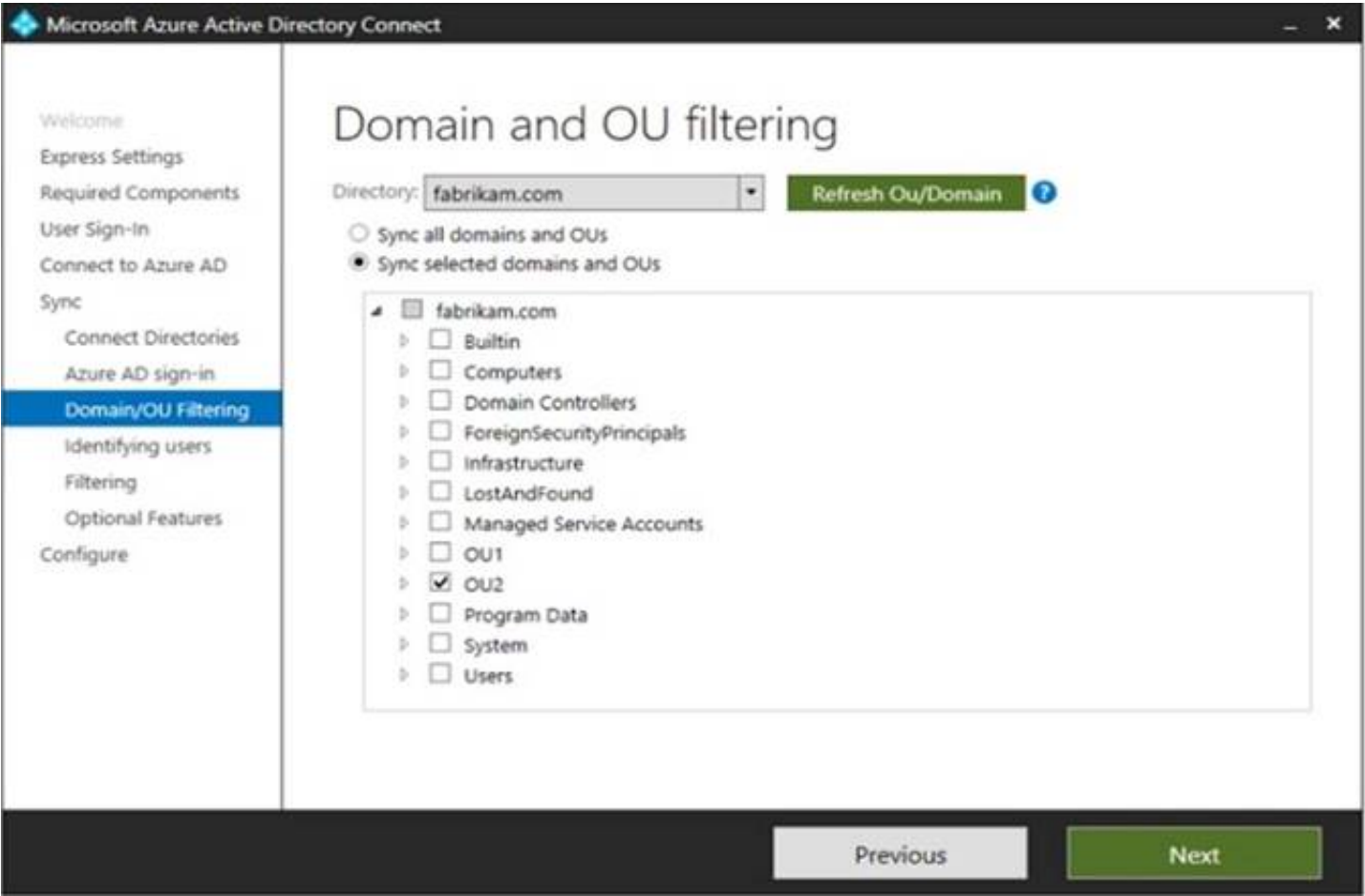
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

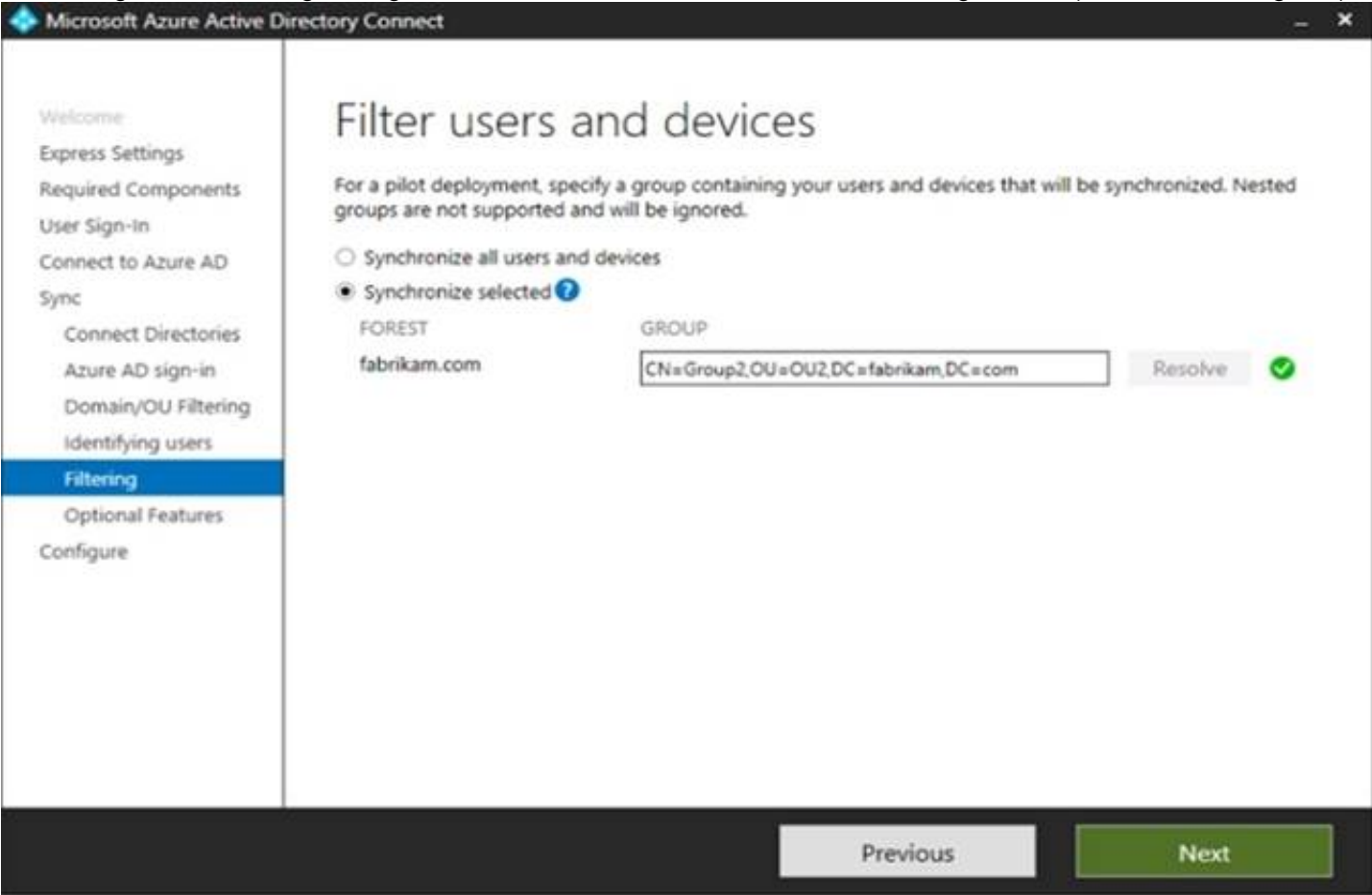
Group	Members
Group1	User1
Group2	User2, User3, Group1

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

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



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



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

Statements	Yes	No
User2 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
Group2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No
 The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

NEW QUESTION 80

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

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

Yes

☐

No

☐

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

☐☐

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

☐☐

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes

Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

NEW QUESTION 82

HOTSPOT - (Topic 6)

HOTSPOT

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

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

The tenant has a conditional access policy that has the following configurations: Name: Policy1
 Assignments:
 - Users and groups: Group1
 - Cloud apps or actions: All cloud apps
 ? Access controls:
 ? Grant, require multi-factor authentication
 ? Enable policy: Report-only
 You set Enabled Security defaults to Yes for the tenant.
 For each of the following settings select Yes, if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
 ? Conditional Access policies can be enabled in report-only mode.
 ? During sign-in, policies in report-only mode are evaluated but not enforced.
 ? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
 ? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

NEW QUESTION 87

HOTSPOT - (Topic 6)
 You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:
 ? MDM user scope: Some
 ? uk.co.certification.simulator.questionpool.PList@184e72e0
 ? MAM user scope: Some
 ? uk.co.certification.simulator.questionpool.PList@184e7360 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 enroll Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 89

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

Message center

New service request

Product feedback

Service health

Answer Area

To report issues regarding a Microsoft 365 service:

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

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 90

- (Topic 6)

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

- A. Yes
- B. No

Answer: A

Explanation:

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

NEW QUESTION 91

HOTSPOT - (Topic 6)

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

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

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

NOTE; Each correct selection is worth one point.

Answer Area

Users that can use SSPR:

User1, User2, and User4 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

Users that must answer security questions to reset their password:

User1 and User2 only

User1 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can use SSPR:

User1, User2, and User4 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

Users that must answer security questions to reset their password:

User1 and User2 only

User1 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

NEW QUESTION 96

HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager. You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen. Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

NEW QUESTION 97

- (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.

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

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

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

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

NEW QUESTION 102

- (Topic 6)

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy. What should you configure?

- A. actions
- B. incident reports
- C. exceptions
- D. user overrides

Answer: D

Explanation:

A DLP policy can be configured to allow users to override a policy tip and report a false positive.

You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.

If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.

Reference:

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

NEW QUESTION 104

- (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 109

HOTSPOT - (Topic 6)

HOTSPOT

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 110

- (Topic 6)

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

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.

You plan to sync contoso.com to an Azure AD tenant.

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

What should you include in the recommendation?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 114

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 tenant

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

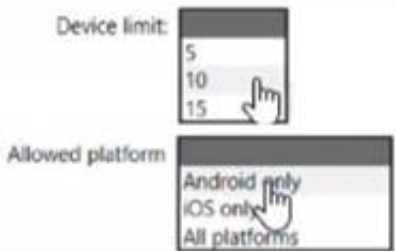
The device type restriction are configured as shown in the following table.

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

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

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

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 119

- (Topic 6)

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

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

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

Another administrator configures the domain to synchronize to Azure AD.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 121

HOTSPOT - (Topic 6)

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

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

? Provision the private store in Microsoft Store for Business.

? Add an app named App1 to the private store.

? Set Private store availability for App1 to Specific groups, and then select Group3.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User3 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can install App1 from the private store.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 126

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 129

- (Topic 6)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.
Does this meet the goal?

- A. Yes

B. No

Answer: A

NEW QUESTION 132

- (Topic 6)

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

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

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

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

Answer: A

NEW QUESTION 136

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

Answer: C

Explanation:

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

Reference:

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

NEW QUESTION 140

- (Topic 6)

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation. You need to run a PowerShell script on the device to collect forensic information.

Which action should you select on the device page?

- A. Initiate Live Response Session
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Go hunt

Answer: A

Explanation:

Reference:

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

NEW QUESTION 145

- (Topic 6)

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

You enable Azure AD Identity Protection.

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

To which role should you add User1?

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

Answer: A

NEW QUESTION 146

HOTSPOT - (Topic 6)

HOTSPOT

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

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

The devices are configured as shown in the following table.

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

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

- 1.Assignments
 - ? Users or workload identities: Group1
 - ? Cloud apps or actions: Office 365 SharePoint Online
 - ? Conditions
 - Filter for devices: Exclude filtered devices from the policy
 - Rule syntax: device.displayName -startsWith "Device"
- 2.Access controls
 - ? Grant
 - Grant: Block access
 - ? Session: 0 controls selected
 - 3.Enable policy: On

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No
 User1 is member of Group1 and has Device1.
 Device1 is not Azure AD joined.
 Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.

Box 2: Yes
 User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.
 Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes
 User2 is member of Group1 and has devices Device2 and Device3.
 Device3 is Android and is Azure AD registered.
 Device3 is excluded from CAPolicy1 (which would block access to Site1).
 Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

NEW QUESTION 151

- (Topic 6)
 You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
 When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

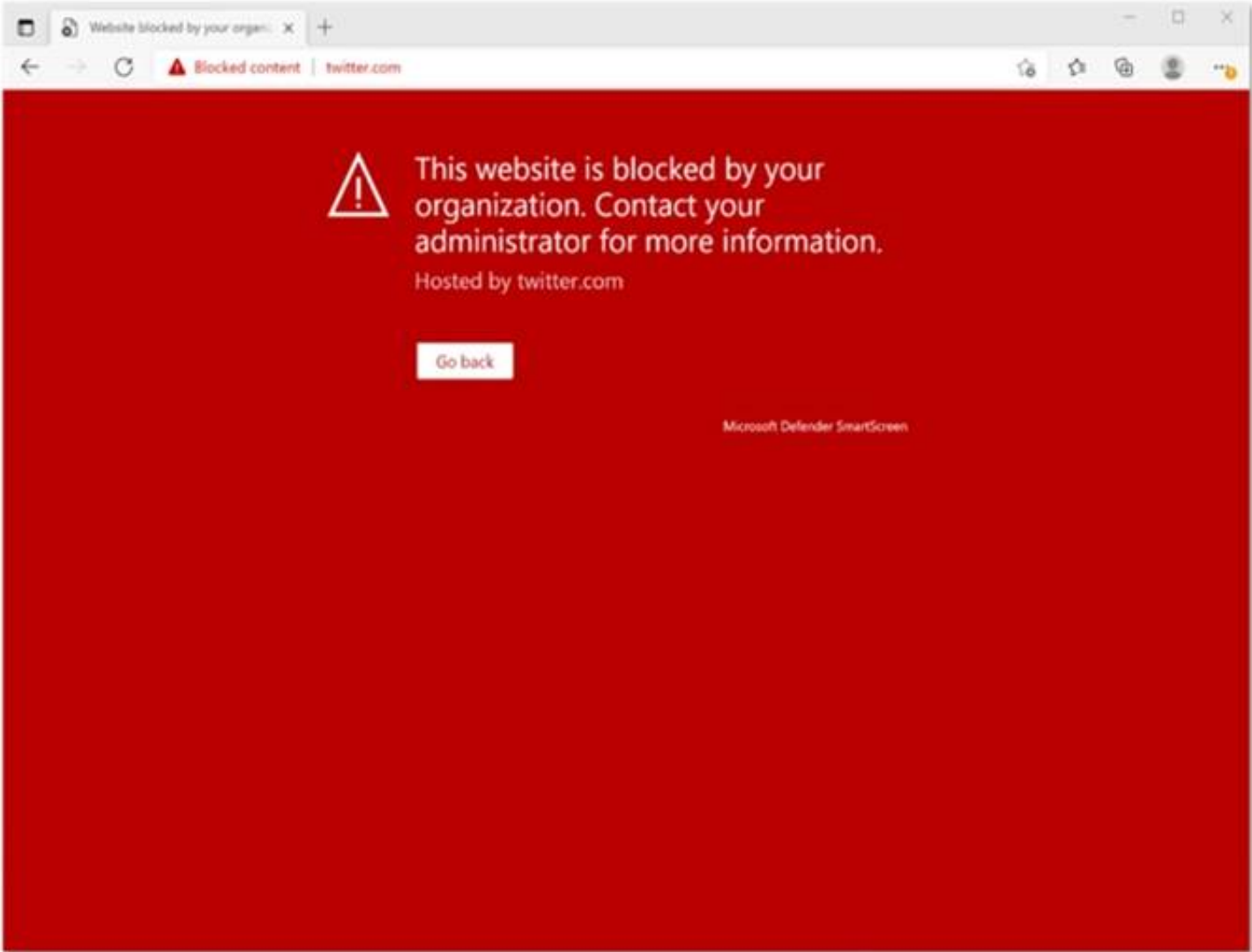


You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

Answer: E

Explanation:



This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference: <https://jadexstrategic.com/web-protection/>

NEW QUESTION 153

- (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 156

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

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 *

App1 policy ✓

What does this policy apply to?

Users and groups

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected ✓

Conditions ⓘ

0 conditions selected

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.

- A. Mastered
- B. Not Mastered

Answer: A

Passing Certification Exams Made Easy

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

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](#)

Name *

App1 policy

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

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

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☒ All users

☐ Select users and groups

⚠ 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.

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

☒

NEW QUESTION 158

HOTSPOT - (Topic 6)

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)

SharePoint

S

Site1

Share

Search Documents

+ New

↑ Upload

✎ Quick edit

↻ Sync

⋮

All Documents

⌵

ⓘ

✎

Documents

Name	Modified	Modified By	+ Add column
File1.docx	About a minute ago	Prvi	
File2.docx	A few seconds ago	Prvi	
File3.docx	A few seconds ago	Prvi	

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Passing Certification Exams Made Easy

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

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

NEW QUESTION 162

DRAG DROP - (Topic 6)

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

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

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Policy Types

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1:

Device2:

Device3:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy Types	Answer Area
App configuration policy	Device1: App protection policy
App protection policy	Device2: Conditional Access policy
Compliance policy	Device3: Compliance policy
Conditional Access policy	

NEW QUESTION 165

- (Topic 6)
 You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.

Policy1

Edit policy

Delete policy

Status

On

Description

Add a description

Severity

Medium

Edit

Category

Information governance

Conditions

Activity is FileModified

Aggregation

Aggregated

Threshold

5 activities

Edit

Window

60 minutes

Scope

All users

Email recipients

User1@M365x082103.onmicrosoft.com

Daily notification limit

25

Edit

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

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

Answer: D

NEW QUESTION 168

- (Topic 6)
 You have a Microsoft 365 E5 subscription.
 Conditional Access is configured to block high-risk sign-ins for all users.
 All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.
 You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.
 What should you configure?

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

Answer: D

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

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

NEW QUESTION 171

- (Topic 6)
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.
You need to deploy the policy. What should you do first?

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

Answer: C

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

NEW QUESTION 173

- (Topic 6)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

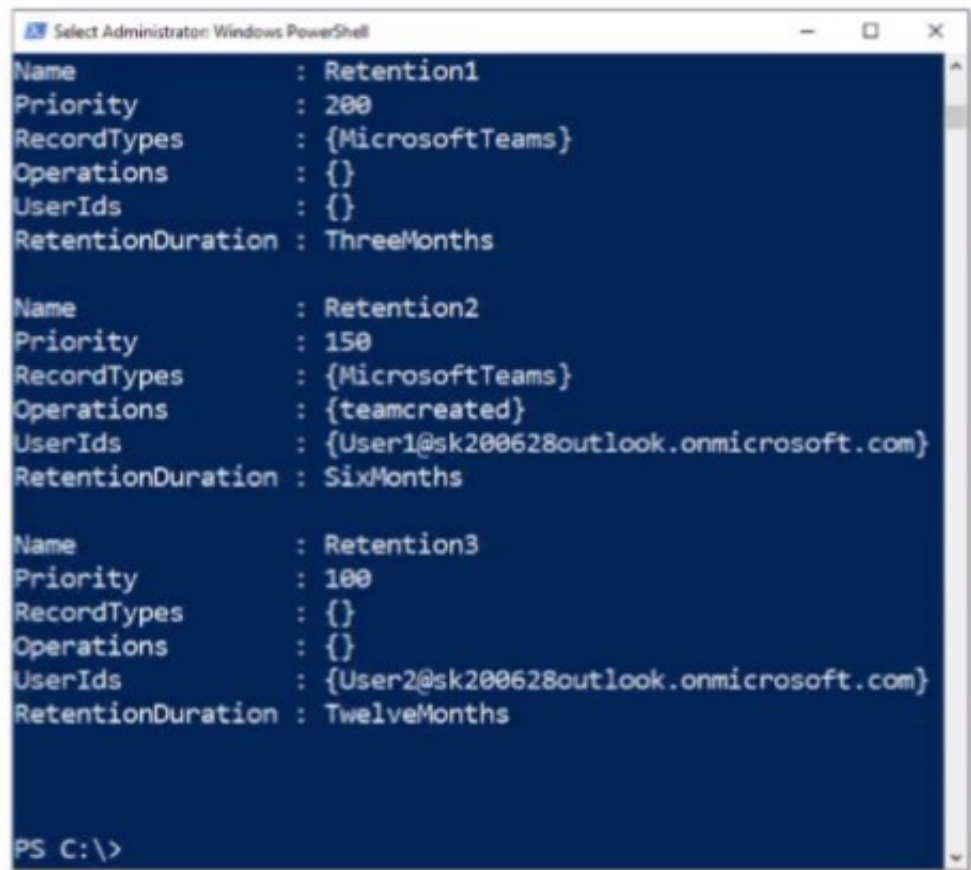
- A. an app configuration policy
- B. an app
- C. a device configuration profile
- D. a device compliance policy

Answer: C

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

NEW QUESTION 177

HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



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

Answer Area

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

not retained

retained for 90 days

retained for six months

retained for one year

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

not retained

retained for 90 days

retained for six months

retained for one year

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

not retained

retained for 90 days

retained for six months

retained for one year

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

not retained

retained for 90 days

retained for six months

retained for one year

NEW QUESTION 181

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 183

- (Topic 6)

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

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

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

Another administrator configures the domain to synchronize to Azure AD.

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

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

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

Reference:

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

NEW QUESTION 188

HOTSPOT - (Topic 6)

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

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

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

NOTE: Each correct selection is worth one point.

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
	lookup		
	project		
	render		
	where		

A. Mastered

B. Not Mastered

Answer: A

Explanation:

AlertInfo
DeviceEvents
DeviceInfo

lookup
project
render
where

ActionType startswith 'ASR'

NEW QUESTION 190
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.
What should you use to onboard each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Device1:

Microsoft Endpoint Manager

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2:

A local script

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1:

Microsoft Endpoint Manager

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2:

A local script

A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

NEW QUESTION 195
- (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 196

- (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 200

HOTSPOT - (Topic 6)

Your company uses Microsoft Defender for Endpoint.

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

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

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

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

Answer Area

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 202

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

What should you configure?

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

Answer: B

Explanation:

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

Sign-in risk policy User risk policy

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

Reference:

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

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

NEW QUESTION 204

- (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 205

FILL IN THE BLANK - (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer Area

Save the audit logs to:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to:

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

NEW QUESTION 209

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

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

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 212

- (Topic 6)

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

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

Azure AD Connect has the following settings:

? Password Hash Sync: Enabled

? Pass-through authentication: Enabled

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

Which users should you identify?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 216

- (Topic 6)

: 241

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 219

- (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 224

- (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 228

- (Topic 6)

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

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

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

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

Answer: D

Explanation:

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

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

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

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

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

Password hash synchronization Pass-through authentication

Active Directory Federation Services

Reference:

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

NEW QUESTION 232

HOTSPOT - (Topic 6)

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured

Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured

Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

NEW QUESTION 237

- (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 242

HOTSPOT - (Topic 6)
 You have a Microsoft 365 E5 subscription.
 You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.
 Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

Sender is condition:

DLP1 only

DLP1 only

DLP2 only

DLP3 only

DLP2 and DLP3 only

DLP1, DLP2, and DLP3

File extension is condition:

DLP1, DLP2, and DLP3

DLP1 only

DLP2 only

DLP3 only

DLP2 and DLP3 only

DLP1, DLP2, and DLP3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Sender is condition:

DLP1 only

DLP1 only

DLP2 only

DLP3 only

DLP2 and DLP3 only

DLP1, DLP2, and DLP3

File extension is condition:

DLP1, DLP2, and DLP3

DLP1 only

DLP2 only

DLP3 only

DLP2 and DLP3 only

DLP1, DLP2, and DLP3

NEW QUESTION 247

HOTSPOT - (Topic 6)
 Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

You create a retention label named Label 1 that has the following configurations:

• Retains content for five years

• Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

• Applies to content that contains the word Merger

• Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention Strue -Force

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 add Exchange email as a location to Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can add the word Acquisition to Policy1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 251

- (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 254

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 256

- (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 260

- (Topic 6)
 You have a Microsoft 365 E5 subscription.
 You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

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

Answer: A

Explanation:

Demonstrate data protection
 Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.
 There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
 In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
 ? From the Security & Compliance tab of your browser, click Home.
 ? Click Data loss prevention > Policy.
 ? Click + Create a policy.
 ? In Start with a template or create a custom policy, click Custom > Custom policy > Next.
 ? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens
 ? Etc.
 Reference:
<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

NEW QUESTION 263

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 268

HOTSPOT - (Topic 6)

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

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer,

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

Answer Area

Solutions

 Catalog

 Audit

 Content search

 Communication compliance

 Data loss prevention

 eDiscovery

▼

 Data lifecycle management

 Information protection

 Information barriers

▼

 Insider risk management

 Records management

 Priva Privacy Risk Managem...

▼

 Priva Subject Rights Requests

 Settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

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

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

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

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

Note: Encryption of data at rest

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

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

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

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

NEW QUESTION 273

- (Topic 6)

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune. Company policy requires that the devices have the following configurations:

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

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

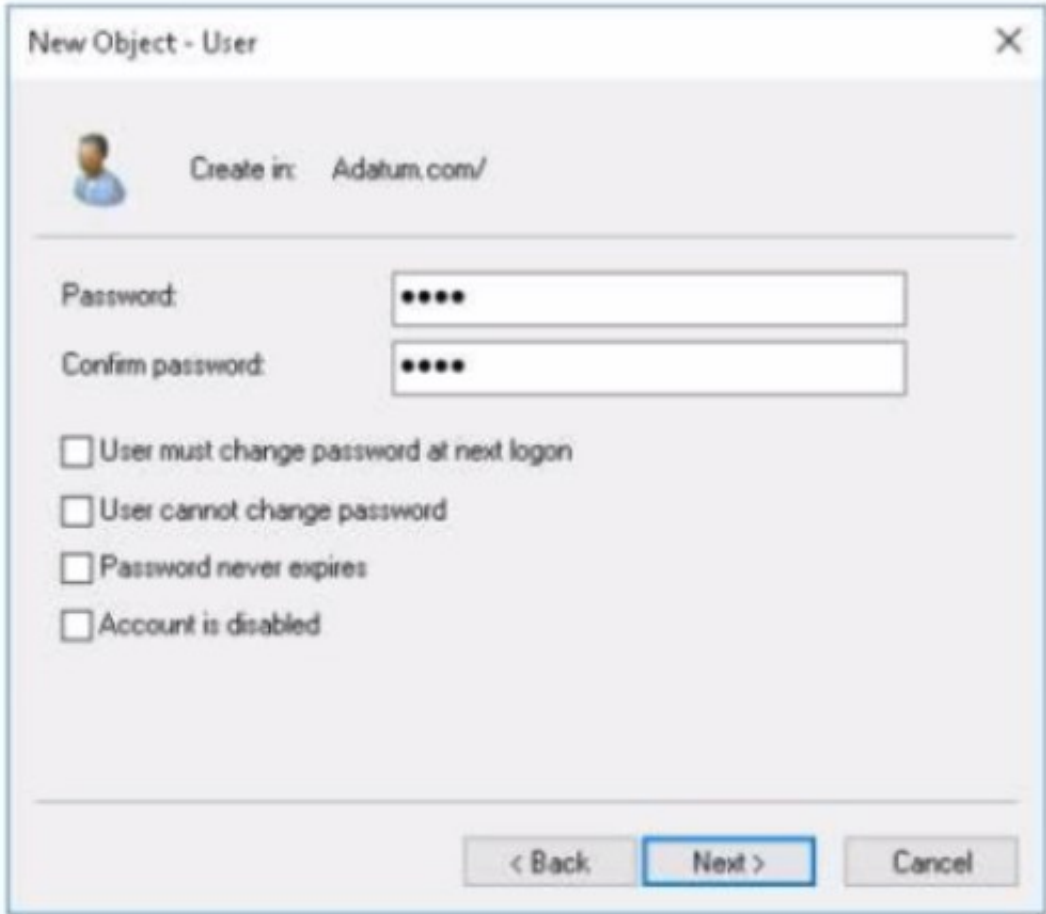
- A. an app configuration policy
- B. a compliance policy
- C a security baseline profile
- D a conditional access policy

Answer: B

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

NEW QUESTION 274

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 278

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 280

HOTSPOT - (Topic 6)

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

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.
What information must be configured for each user before the user can perform a self- service password reset? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User1:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User2:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User3:

Security questions only
Email address only
Phone number only
Security questions only
Phone number and email address

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User2:

Phone number and email address
Email address only
Phone number only
Security questions only
Phone number and email address

User3:

Security questions only
Email address only
Phone number only
Security questions only
Phone number and email address

NEW QUESTION 283

- (Topic 6)
You purchase a new computer that has Windows 10, version 21H1 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

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

Answer: C

NEW QUESTION 288

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 292

- (Topic 6)

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

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

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

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

- A. Yes
- B. No

Answer: A

NEW QUESTION 296

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 301

HOTSPOT - (Topic 6)
HOTSPOT

You have a Microsoft 365 E3 subscription.
You plan to launch Attack simulation training for all users.
Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Social engineering technique:

Credential harvest

Link to malware

Malware attachment

Training experience:

Identity Theft

Mass Market Phishing

Web Phishing

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Credential Harvest
Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.
Note: In Attack simulation training, multiple types of social engineering techniques are available:
Credential Harvest
Malware Attachment
Link to Malware
Etc.
Box 2: Mass Market Phishing

NEW QUESTION 302

- (Topic 6)
You have a Microsoft 365 E5 tenant.
The Microsoft Secure Score for the tenant is shown in the following exhibit.

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

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

↓ Export	12 items	🔍 Search	⌵ Filter	{≡ Group by ▾
Applied filters:				
Rank ⓘ	Improvement action	Score impact	Points achieved	
1	Require MFA for administrative roles	+16.95%	0/10	
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9	
3	Enable policy to block legacy authentication	+13.56%	0/8	
4	Turn on user risk policy	+11.86%	0/7	
5	Turn on sign-in risk policy	+11.86%	0/7	
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4	
7	Enable self-service password reset	+1.69%	0/1	
8	Turn on customer lockbox feature	+1.69%	0/1	
9	Use limited administrative roles	+1.69%	0/1	
10	Designate more than one global admin	+1.69%	0/1	

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

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

Answer: ABC

Explanation:

Reference:

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

NEW QUESTION 304

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 onboard to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

NEW QUESTION 305

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

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

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

The default shared folder location for User1 is:

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

The default Office theme for User 2 is:

▼
Colorful
Dark Gray
White

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_1

The default Office theme for User 2 is:

Colorful

Dark Gray

White

NEW QUESTION 308

- (Topic 6)
You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again. When will File1.docx be deleted automatically?

- A. January 1,2023
- B. January 1,2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

Answer: D

Explanation:

Retention wins over deletion. Note:
Explanation for the four different principles:
* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system- initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
* 2. Etc. Reference:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

NEW QUESTION 313

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 317

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

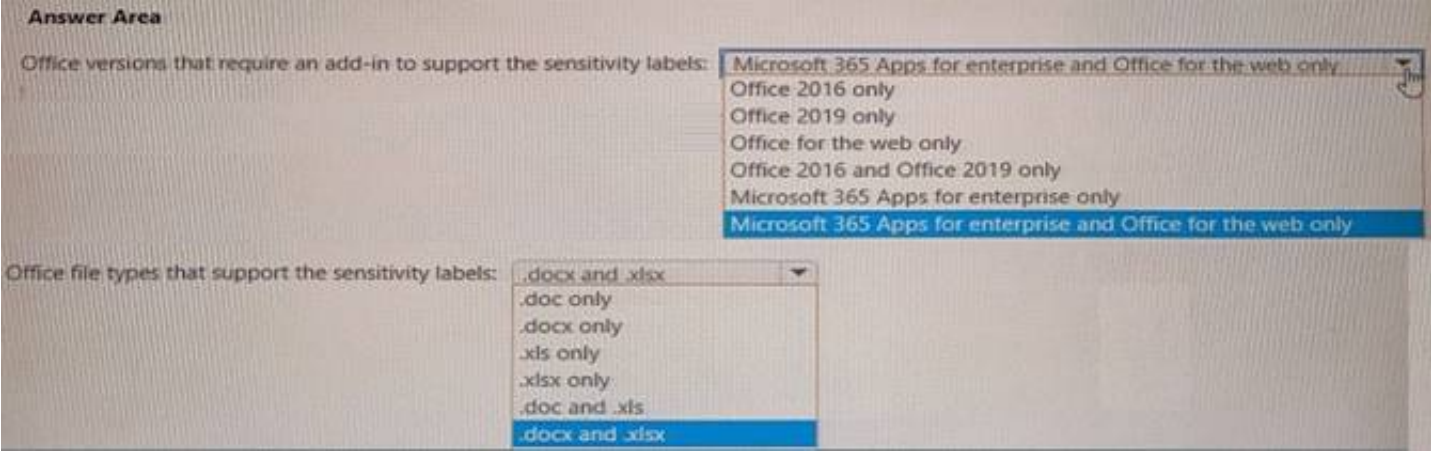
The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- .xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

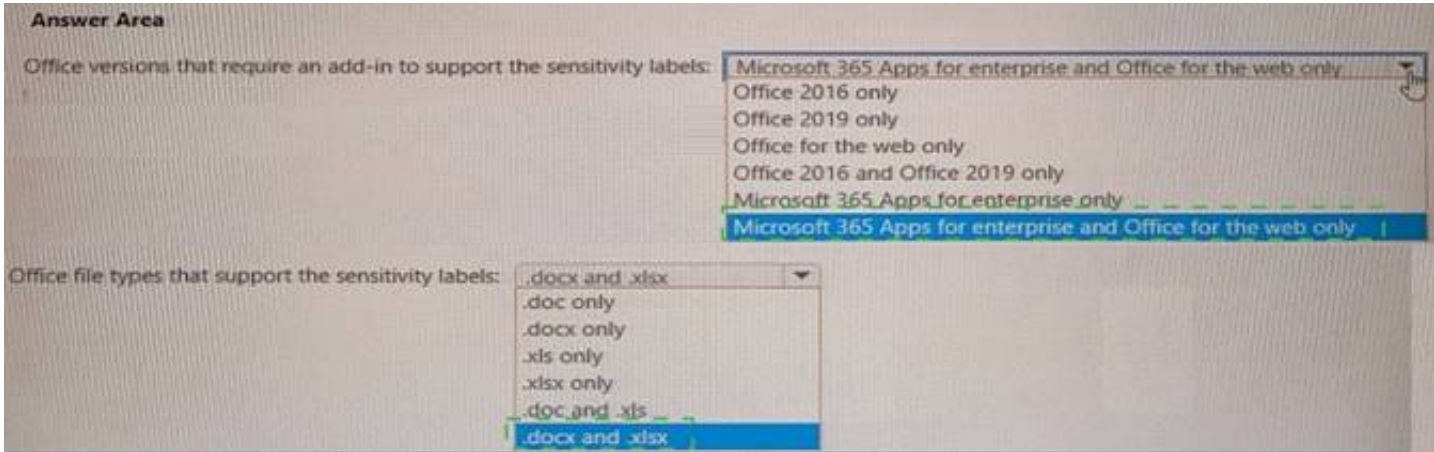
What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 321

HOTSPOT - (Topic 6)

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

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

- ? Name: AutoLabel1
 - ? Label to auto-apply: Sensitivity1
 - ? Rules for SharePoint Online sites: Rule1-SPO
 - ? Choose locations where you want to apply the label: Site1
- Rule1-SPO is configured as shown in the following exhibit.

Edit rule

Name *

Rule1-SPO

Description

Rule1 description

^ Conditions

We'll apply this policy to content that matches these conditions.

^ Content contains sensitive info types

Default

All of these

Sensitive info types

IP Address Accuracy 85 to 100 Instance count 2 to Any

Add

Create group

+ Add condition

Save

Cancel

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 File1.docx.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 325

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 327

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 331

- (Topic 5)
You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.
What should you do?

- A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
- B. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.
- C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
- D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

NEW QUESTION 333

HOTSPOT - (Topic 4)
HOTSPOT
You create the Microsoft 365 tenant.
You implement Azure AD Connect as shown in the following exhibit.

DNS for that domain.

Note:

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

Text (TXT)

Mail exchanger (MX)

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

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

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

NEW QUESTION 342

- (Topic 4)

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

Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication

B. pass-through authentication and seamless SSO

C. password hash synchronization and seamless SSO

D. password hash synchronization

Answer: C

Explanation:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

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

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

Fabrikam does NOT plan to implement identity federation.

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

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

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

Reference:

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

NEW QUESTION 347

HOTSPOT - (Topic 3)

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Number of required policies:

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Number of required policies:

NEW QUESTION 349

HOTSPOT - (Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.

To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 security center	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 security center	

NEW QUESTION 353

- (Topic 3)

You need to configure Office on the web to meet the technical requirements. What should you do?

- A. Assign the Global reader role to User1.
- B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
- C. Configure an auto-labeling policy to apply the sensitivity labels.
- D. Assign the Office apps admin role to User1.

Answer: B

Explanation:

Reference:

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

NEW QUESTION 358

- (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 361

- (Topic 2)

You need to meet the technical requirement for the EU PII data. What should you create?

- A. a retention policy from the Security & Compliance admin center.
- B. a retention policy from the Exchange admin center
- C. a data loss prevention (DLP) policy from the Exchange admin center
- D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies>

EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION 363

HOTSPOT - (Topic 2)

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

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

▼
Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by:

▼
Activity
Detail
Item
User agent

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 364

- (Topic 1)

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

- A. User2
- B. User3
- C. User4
- D. User5

Answer: C

Explanation:

References:

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

NEW QUESTION 367

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 370

- (Topic 1)

On which server should you install the Azure ATP sensor?

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

Answer: A

Explanation:

References:

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

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

NEW QUESTION 371

- (Topic 1)

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

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

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

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

You configure a pilot for co-management.

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

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

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD- join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager <https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client>

NEW QUESTION 376

HOTSPOT - (Topic 1)

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

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

New

×

Info

Name

Policy1

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On

Off

Conditions

×

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Device state (preview)

×

Info

Configure

Yes

No

Include

Exclude

Select the device state condition used to exclude devices from policy.

Device Hybrid Azure AD joined

Device marked as compliant

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 377

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 379

- (Topic 1)
You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

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

Passing Certification Exams Made Easy

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

D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:

References:

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

NEW QUESTION 381

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 385

- (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 387

.....

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 First Try
- * MS-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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