

Microsoft.MS-102.vJan-2024.by.Dary.148q

Number: MS-102
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: MS-102

Exam Name: Microsoft 365 Administrator



Case 01

Overview

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide. Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment

Active Directory Environment

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS.

All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements

Planned Changes

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

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 will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

Application Requirements

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements

Fabrikam identifies the following security requirements:

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

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

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

The principle of least privilege must be used.

QUESTION 1

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.

Correct Answer: A

Section:

QUESTION 2

HOTSPOT

You need to ensure that Admin4 can use SSPR.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

Answer Area:

Answer Area

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

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

Section:

Explanation:

QUESTION 3

Which role should you assign to User1?

Available Choices (select all choices that are correct)

A. Hygiene Management



- B. Security Reader
- C. Security Administrator
- D. Records Management

Correct Answer: C

Section:

Explanation:

QUESTION 4

HOTSPOT

You create the Microsoft 365 tenant.

You implement Azure AD Connect as shown in the following exhibit.

Azure Active Directory admin center




Home > Azure AD Connect

Azure AD Connect




Azure Active Directory

Troubleshoot Refresh

SYNC STATUS

	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	Disabled	0 domains
	Pass-through authentication	Disabled	0 agents

vdumps

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.

Hot Area:

Answer Area

During Project1, sales department users can access [answer choice] applications by using SSO.

both on-premises and cloud-based
only cloud-based
only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

both on-premises and in the cloud
in the cloud only
on-premises only

Answer Area:

Answer Area

During Project1, sales department users can access [answer choice] applications by using SSO.

both on-premises and cloud-based
only cloud-based
only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

both on-premises and in the cloud
in the cloud only
on-premises only

Section:

Explanation:

QUESTION 5

HOTSPOT

You are evaluating the use of multi-factor authentication (MFA).

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes **No**

Users will have 14 days to register for MFA after they sign in for the first time.

Users must use the Microsoft Authenticator app to complete MFA.

After registering, users must use MFA for every sign-in.

Answer Area:

Answer Area

Statements

Yes **No**

Users will have 14 days to register for MFA after they sign in for the first time.

Users must use the Microsoft Authenticator app to complete MFA.

After registering, users must use MFA for every sign-in.



Section:

Explanation:

QUESTION 6

You need to configure just in time access to meet the technical requirements. What should you use?

- A. entitlement management
- B. Azure AD Privileged Identity Management (PIM)
- C. access reviews
- D. Azure AD Identity Protection

Correct Answer: B

Section:

QUESTION 7

HOTSPOT

You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements. What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure the notifications:

Briefing email	▼
Briefing email	
Help desk information	
Organization information	

To limit access:

Release preferences	▼
Privileged Access	
Release preferences	
Office installation options	

Answer Area:

Answer Area

To configure the notifications:

Briefing email	▼
Briefing email	
Help desk information	
Organization information	

To limit access:

Release preferences	▼
Privileged Access	
Release preferences	
Office installation options	

Section:

Explanation:

QUESTION 8

You are evaluating the required processes for Project1.

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

Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. alias (CNAME)

Correct Answer: D

Section:

Explanation:

QUESTION 9

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

Correct Answer: C

Section:

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.

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

QUESTION 10

HOTSPOT

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.

Hot Area:

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

Answer Area:

Answer Area

Users:

- Admin1 only
- Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade:

- Reports
- Service Health**
- Message center

Section:

Explanation:

Case 02

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements.

If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

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

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com.

Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.

Devices without an assigned compliance policy show a status of Compliant.

User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.

Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.

Requirements

Planned Changes

Litware plans to implement the following changes:

Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.

Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.

Implement data loss prevention (DLP) policies to protect confidential information.

Grant User2 permissions to review the audit logs of the litware.com tenant.

Deploy new devices to the Seattle office as shown in the following table.



Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

Implement a notification system for when DLP policies are triggered.

Configure a Safe Attachments policy for the litware.com tenant.

Technical Requirements

Litware identifies the following technical requirements:

Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.

Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.

All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.

Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.

A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.

User2 must be granted the permissions to review audit logs for the following activities:

- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD

Users must be able to apply sensitivity labels to documents by using Office for the web.

Windows Autopilot must be used for device provisioning, whenever possible.

A DLP policy must be created to meet the following requirements:

- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.

- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.

The principle of least privilege must be used.

QUESTION 1

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements.

What should you do?

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 2

You need to configure the compliance settings to meet the technical requirements.

What should you do in the Microsoft Endpoint Manager admin center?

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 3

HOTSPOT

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.

Hot Area:

Role group: ▼

Reviewer
Global reader
Data Investigator
Compliance Management

Tool: ▼

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

Answer Area:

Role group: ▼

Reviewer
Global reader
Data Investigator
Compliance Management

Tool: ▼

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



Section:

Explanation:

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

QUESTION 4

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.

Correct Answer: B

Section:

Explanation:

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

QUESTION 5

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 6

HOTSPOT

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.

Hot Area:

Answer Area


The screenshot shows a configuration interface with two main sections. The first section is labeled "Policy type:" and contains a dropdown menu with four options: "Retention", "Label", "Retention", and "Auto-labeling". The "Retention" option is currently selected. The second section is labeled "Number of required policies:" and contains a dropdown menu with three options: "1", "2", and "3". The "2" option is currently selected. A large "Vdumps" watermark is overlaid on the right side of the image.

Answer Area:

Answer Area

Policy type: 

Label
Retention
Auto-labeling

Number of required policies: 

1
2
3

Section:

Explanation:

QUESTION 7

HOTSPOT

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Configure:

Device configuration profiles Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group:

<input type="text"/> 
UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Answer Area:

Configure: ▼

Device configuration profiles Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group: ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Section:

Explanation:

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

QUESTION 8

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

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



Correct Answer: D

Section:

Explanation:

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

QUESTION 9

HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Supported devices:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2, and Device3	
Device1, Device4, and Device5	
Device1, Device2, Device3, Device4, and Device5	

Number of required profiles:

	▼
1	
2	
3	
4	
5	

Answer Area:

Supported devices:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2, and Device3	
Device1, Device4, and Device5	
Device1, Device2, Device3, Device4, and Device5	

Number of required profiles:

	▼
1	
2	
3	
4	
5	

Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create>

Exam D

QUESTION 1

You have a Microsoft 365 subscription.

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

- A. Yes
- B. No

Correct Answer: B
Section:

QUESTION 2

DRAG DROP

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

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

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

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

<https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>

Select and Place:

Actions

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

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

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

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

Answer Area



Correct Answer:

Actions

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

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

Answer Area

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

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.



Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>

QUESTION 3

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

You need to create a detection exclusion in Azure ATP.

Which tool should you use?

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

Correct Answer: D

Section:

Explanation:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

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

QUESTION 4

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



Correct Answer: B

Section:

Explanation:

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

QUESTION 5

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

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

You have a Microsoft 365 E5 subscription.

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

You need to ensure that SecAdmin1 can manage 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

Correct Answer: A

Section:

QUESTION 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 Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

You need to assign the Security Administrator role.

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

QUESTION 7

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

You need to assign the Security Administrator role.

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

QUESTION 8

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

Correct Answer: C

Section:

Explanation:

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



QUESTION 9

You have a Microsoft 365 E5 tenant.

You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.

You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

- * Minimizes user interaction
- * Minimizes administrative effort
- * Automatically installs corporate apps

What should you recommend?

- A. Automated Device Enrollment (ADE)
- B. bring your own device (BYOD) user and device enrollment
- C. Apple Configurator enrollment

Correct Answer: A

Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll>

QUESTION 10

HOTSPOT

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

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

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

Hot Area:

Add apps to the private store:

<input type="checkbox"/>	User3 only
<input type="checkbox"/>	User2 and User3 only
<input type="checkbox"/>	User1 and User3 only
<input type="checkbox"/>	User1, User2 and User3 only
<input type="checkbox"/>	User1, User2, User3, and User4

Install apps from the private store:

<input type="checkbox"/>	User3 only
<input type="checkbox"/>	User2 and User3 only
<input type="checkbox"/>	User1 and User3 only
<input type="checkbox"/>	User2, User3 and User4 only
<input type="checkbox"/>	User1, User2, User3, and User4

Answer Area:

Add apps to the private store:

▼
User3 only
User2 and User3 only
User1 and User3 only
User1, User2 and User3 only
User1, User2, User3, and User4

Install apps from the private store:

▼
User3 only
User2 and User3 only
User1 and User3 only
User2, User3 and User4 only
User1, User2, User3, and User4

Section:

Explanation:

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

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

QUESTION 11

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 12

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



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

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 13

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 14

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 15



HOTSPOT

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

Data Transfer

Backup org data to Android backup services ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Send org data to other apps ⓘ	Policy managed apps
Select apps to exempt	Select
Save copies of org data ⓘ	<input type="radio"/> Allow <input checked="" type="radio"/> Block
Allow user to save copies to selected services ⓘ	SharePoint
Transfer telecommunication data to ⓘ	Any dialer app
Dialer App Package ID	
Dialer App Name	
Receive data from other apps ⓘ	All Apps
Open data into Org documents ⓘ	<input type="radio"/> Allow <input type="radio"/> Block
Allow users to open data from selected services ⓘ	3 selected
Restrict cut, copy, and paste between other apps ⓘ	Policy managed apps with paste in
Screen capture and Google Assistant ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Approved keyboards ⓘ	<input type="radio"/> Require <input checked="" type="radio"/> Not required
Select keyboards to approve	Select

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

Hot Area:

Answer Area

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

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

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

any app
any app
only managed apps
only unmanaged apps

Answer Area:
Answer Area

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

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

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

any app
any app
only managed apps
only unmanaged apps



Section:

Explanation:

QUESTION 16

HOTSPOT

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

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

You are implementing Microsoft Defender for Endpoint

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

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

NOTE Each correct selection is worth one point.

Hot Area:

Answer Area

Users that can enable RBAC:

- Admin1 only
- Admin1 and Admin2 only**
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

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

- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only**

Answer Area:
Answer Area

Users that can enable RBAC:

- Admin1 only
- Admin1 and Admin2 only**
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

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

- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only**

Section:
Explanation:

QUESTION 17

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps. You need to be notified when a single user downloads more than 50 files during any 60-second period. What should you configure?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an anomaly detection policy

Correct Answer: D
Section:

QUESTION 18

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

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

Hot Area:

Answer Area

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



Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 19

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

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 20

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.

What should you use?

- A. Active users in the Microsoft 365 admin center
- B. Reports in Microsoft Purview compliance portal
- C. the Licenses blade in the Microsoft Entra admin center
- D. Reports in the Microsoft 365 admin center

Correct Answer: D

Section:

Explanation:

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.



Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No ¹	No ¹	No ¹	No ¹
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

QUESTION 21

HOTSPOT

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

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

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

(user.userType

- eq "Guest"
- in "Guest"
- ne "Guest"
- notmatch "Member"

- contains "Support"
- in "Support"
- match "Support"
- startsWith "Sup"

Answer Area:

Answer Area

(user.userType

- eq "Guest"
- in "Guest"
- ne "Guest"
- notmatch "Member"

- contains "Support"
- in "Support"
- match "Support"
- startsWith "Sup"

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

QUESTION 22

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.

Hot Area:

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

Answer Area:
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

Section:
Explanation:
<https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time>

QUESTION 23
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

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

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

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

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

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

What is the minimum number of deployment groups required?

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

Correct Answer: C

Section:

Explanation:

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

Note: What are Deployment Groups?

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

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

QUESTION 24

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

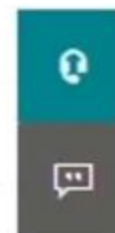
Issue title	Affected service	Issue type
> Microsoft service health (6)		
Issues in your environment that require action (0)		



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

Correct Answer: B

Section:

Explanation:

QUESTION 25

HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

Scope type: Directory

Selected members: Group1

Assignment type: Active

Assignment starts: Mar 15, 2023

Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

Scope type: Directory

Selected members: Group2

Assignment type: Eligible

Assignment starts: Jun 15, 2023

Assignment ends: Oct 15, 2023

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Statements

On July 15, 2023, Admin1 can reset the password of a user.

Yes

No

On June 20, 2023, Admin2 can manage Microsoft Exchange Online.

On May 1, 2023, Admin3 can reset the password of a user.

Answer Area:

Answer Area

Statements

On July 15, 2023, Admin1 can reset the password of a user.

Yes

No

On June 20, 2023, Admin2 can manage Microsoft Exchange Online.

On May 1, 2023, Admin3 can reset the password of a user.

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member-owner>

QUESTION 26

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

Correct Answer: B

Section:

Explanation:

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.
<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

QUESTION 27

HOTSPOT

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

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

Can be added to Compliance1 as recipients of noncompliance notifications

Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Answer Area:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Section:

Explanation:

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/>

QUESTION 28

HOTSPOT

You have a Microsoft 365 E5 tenant.

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

Compliance settings [Edit](#)

Microsoft Defender ATP

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

Device Health

Rooted devices
Require the device to be at or under the Device Threat Level **Block**

System Security

Require a password to unlock mobile devices **Require**
Required password type **Device default**
Encryption of data storage on device. **Require**
Block apps from unknown sources **Block**

Actions for noncompliance [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately



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

Hot Area:

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

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

Rooted devices will be

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

Answer Area:

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

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

Rooted devices will be

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android>

QUESTION 29

You have a Microsoft 365 E5 tenant.

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

Review your settings

Name [Edit](#)
Retention1

Description for admins [Edit](#)

Description for users [Edit](#)

File plan descriptors [Edit](#)
Reference Id: 1
Business function/department Legal
Category: Compliance
Authority type: Legal

Retention [Edit](#)
7 years
Retain only
Based on when it was created

[Back](#) [Create this label](#) [Cancel](#)

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 30

You have the sensitivity labels shown in the following exhibit.



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	Prvi	04/24/2020
- Label2	1	Prvi	04/24/2020
Label3	0-highest	Prvi	04/24/2020
Label4	0-highest	Prvi	04/24/2020
- Label5	5	Prvi	04/24/2020
Label6	0-highest	Prvi	04/24/2020



Which labels can users apply to content?

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 31

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

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

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

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

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

Correct Answer: C

Section:

QUESTION 32

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

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. yes
- B. No



Correct Answer: B

Section:

QUESTION 33

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

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.

Does this meet the goal?

- A. yes
- B. No

Correct Answer: A

Section:

QUESTION 34

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

correct solution, while others might not have a correct solution.

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

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

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

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

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

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

A. yes

B. No

Correct Answer: A

Section:

QUESTION 35

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.

You have the devices shown in the following table.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

Vdumps

You plan to enable co-management.

You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

A. Device1 only

B. Device2 only

C. Device3 only

D. Device2 and Device3 only

E. Device1, Device2, and Device3

Correct Answer: D

Section:

QUESTION 36

HOTSPOT

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show time limit error when installation takes longer than specified number of minutes.	<input type="text" value="60"/>
Show custom message when time limit error occurs.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow users to collect logs about installation errors.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Only show page to devices provisioned by out-of-box experience (OOBE)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Block device use until all apps and profiles are installed	<input type="radio"/> Yes <input checked="" type="radio"/> No

You assign the policy to Group1.

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.

Hot Area:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

Answer Area:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

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

QUESTION 37

HOTSPOT

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/discovery>

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.

Hot Area:

 Vdumps

Statements

Yes

No

If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.

If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.

If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.

Answer Area:

Statements

Yes

No

If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.

If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.

If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.

Section:

Explanation:

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



QUESTION 38

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week.

What should you do from the Security & Compliance admin center?

- A. Perform a content search
- B. Create a supervision policy
- C. Create an eDiscovery case
- D. Perform an audit log search

Correct Answer: D

Section:

QUESTION 39

HOTSPOT

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

Choose the types of content to protect

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

Content contains

Any of these ▾

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

Retention labels

1 year ✕

Add ▾

+ Add group

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

NOTE: Each correct selection is worth one point.

Hot Area:

DLP1 cannot be applied to [answer choice].

Exchange email
SharePoint sites
OneDrive accounts

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

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

Answer Area:

DLP1 cannot be applied to [answer choice].

	▼
Exchange email	
SharePoint sites	
OneDrive accounts	

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

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy>

QUESTION 40

HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point.



Hot Area:

In Azure:

	▼
Add and configure the Diagnostics settings for the Azure Activity Log.	
Add and configure an Azure Log Analytics workspace.	
Add an Azure Storage account and Azure Cognitive Search	
Add an Azure Storage account and a file share.	

On the computers:

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

Answer Area:

In Azure:

	▼
Add and configure the Diagnostics settings for the Azure Activity Log.	
Add and configure an Azure Log Analytics workspace.	
Add an Azure Storage account and Azure Cognitive Search	
Add an Azure Storage account and a file share.	

On the computers:

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer>

QUESTION 41

You enable the Azure AD Identity Protection weekly digest email.

You create the users shown in the following table.



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

Which users will receive the weekly digest email automatically?

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

Correct Answer: E

Section:

Explanation:

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or

Security Administrators will automatically be added to the recipients list.

QUESTION 42

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

Correct Answer: B
Section:

QUESTION 43

HOTSPOT
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
A user named User1 stores documents in Microsoft OneDrive.
You need to place the contents of User1's OneDrive account on an eDiscovery hold.
Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



https://	<input type="text"/>	<input type="text"/>	<input type="text"/>
	onedrive.live.com/	User1	
	contoso.onmicrosoft.com/	Sites/User1	
	contoso.sharepoint.com/	contoso_onmicrosoft_com/User1	
	contoso-my.sharepoint.com/	personal/User1_contoso_onmicrosoft_com	

Answer Area:

https://	<input type="text"/>	<input type="text"/>	<input type="text"/>
	onedrive.live.com/	User1	
	contoso.onmicrosoft.com/	Sites/User1	
	contoso.sharepoint.com/	contoso_onmicrosoft_com/User1	
	contoso-my.sharepoint.com/	personal/User1_contoso_onmicrosoft_com	

Section:
Explanation:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds>

QUESTION 44

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.

Hot Area:

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"/>

Answer Area:

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only>

QUESTION 45

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Block emails that contain financial data.

Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

Use the following location: Exchange email.

Display the following policy tip text: Message contains sensitive data.

When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result 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.

Select and Place:

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

Result

When the user sends an email that contains only financial data:

Result



Correct Answer:

Results

The email will be allowed, and the user will receive the policy tip: Message blocked.
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.
The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data:

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>



QUESTION 46

DRAG DROP

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

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

You use Azure Information Protection.

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

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

Select and Place:

Actions

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

Answer Area

Correct Answer:

Actions

-
-
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
-
- Run GenConnectorConfig.ps1 on Server2.

Answer Area

- Install the Microsoft Rights Management connector on Server2.
- Authorize Server1.
- Run GenConnectorConfig.ps1 on Server1.

Section:

Explanation:

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

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

QUESTION 47

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

- A. Device1, Device4, and Device6
- B. Device2, Device3, and Device5
- C. Device1, Device2, Device3, and Device6
- D. Device1, Device2, Device4, and Device5

Correct Answer: C

Section:

Explanation:

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

<https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

**QUESTION 48**

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.

Hot Area:

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"/>

Answer Area:

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"/>

Section:

Explanation:

QUESTION 49

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule
- B. an allowed/blocked list rule
- C. an alert suppression rule

D. an indicator

Correct Answer: D

Section:

Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

QUESTION 50

HOTSPOT

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

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

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



New audit retention policy



Name *

Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

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

Users:

Admin1 ×

Duration *

90 Days

6 Months

1 Year

Priority *

100

Save

Cancel

After Policy1 is created, the following actions are performed:

Admin1 creates a user named User1.

Admin2 creates a user named User2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Vdumps

User1:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

Answer Area:

User1:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

Section:

Explanation:

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

QUESTION 51

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.





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

- A. 20 hours
- B. 12 hours
- C. 7 hours
- D. 48 hours

Correct Answer: B
Section:

QUESTION 52
HOTSPOT

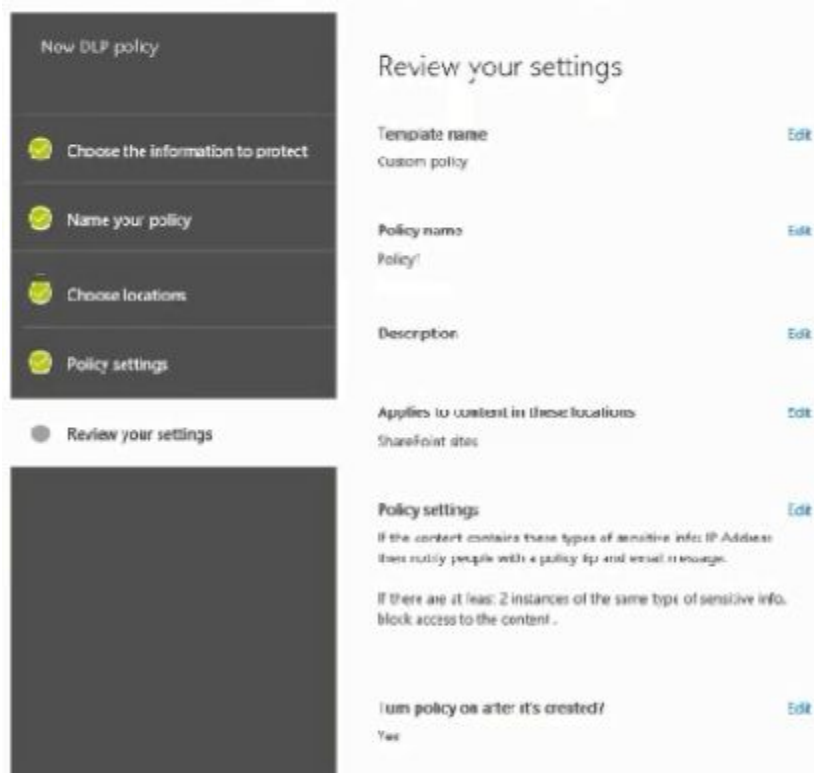
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has the files in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.docx	2
File4.bmp	3
File5.doc	3

The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data loss prevention (DLP) policy named Policy1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User 1:	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

User 2:	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

Answer Area:

Answer Area

User 1:	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input checked="" type="checkbox"/>

User 2:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

Section:

Explanation:

QUESTION 53

You have a Microsoft 365 F5 subscription.

You plan to deploy 100 new Windows 10 devices.

You need to order the appropriate version of Windows 10 for the new devices. The version must

Meet the following requirements.

Be serviced for a minimum of 24 months.

Support Microsoft Application Virtualization (App-V)

Which version should you identify?

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

Correct Answer: D

Section:

Explanation:

<https://docs.microsoft.com/en-us/windows/release-health/release-information>

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

QUESTION 54

HOTSPOT

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

You have devices enrolled in Intune as shown in the following table.

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

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

NOTE: Each correct selection is worth one point.



Hot Area:

Device1:

No profiles
Profile1 only
Profile4 only
Profile1 and Profile4 only
Profile1, Profile1, and Profile4 only

Device2:

No profiles
Profile1 only
Profile2 only
Profile3 only
Profile1 and Profile2 only
Profile2 and Profile3 only

Answer Area:

Device1:

No profiles
Profile1 only
Profile4 only
Profile1 and Profile4 only
Profile1, Profile1, and Profile4 only

Device2:

No profiles
Profile1 only
Profile2 only
Profile3 only
Profile1 and Profile2 only
Profile2 and Profile3 only



Section:

Explanation:

QUESTION 55

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

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

What should you create?

- A. scope tags

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 56

HOTSPOT

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.



Hot Area:

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"/>

Answer Area:

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"/>

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability>

QUESTION 57

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 58

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2



You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Show app and profile configuration progress: Yes

Allow users to collect logs about installation errors: Yes

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

Assignments: Group2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements

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

Yes **No**

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

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

Answer Area:

Statements

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

Yes **No**

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

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

Section:

Explanation:

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

QUESTION 59

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

Correct Answer: A

Section:

Explanation:

<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>

QUESTION 60

You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.



Anti-malware policy - Internet Explorer

Default

general

settings

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

No

Yes and use the default notification text

Yes and use custom notification text

*Custom notification text:

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

Off

On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

+ -

FILE TYPES

- .ace**
- .ani
- .app
- .docm

Notifications

Sender Notifications

Sends a message to the sender of the undelivered message.

Notify internal senders

Notify external senders

Administrator Notifications

Sends a message to the administrator of the undelivered message.

Notify administrator about undelivered messages from internal senders

Save Cancel

100%

An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 61

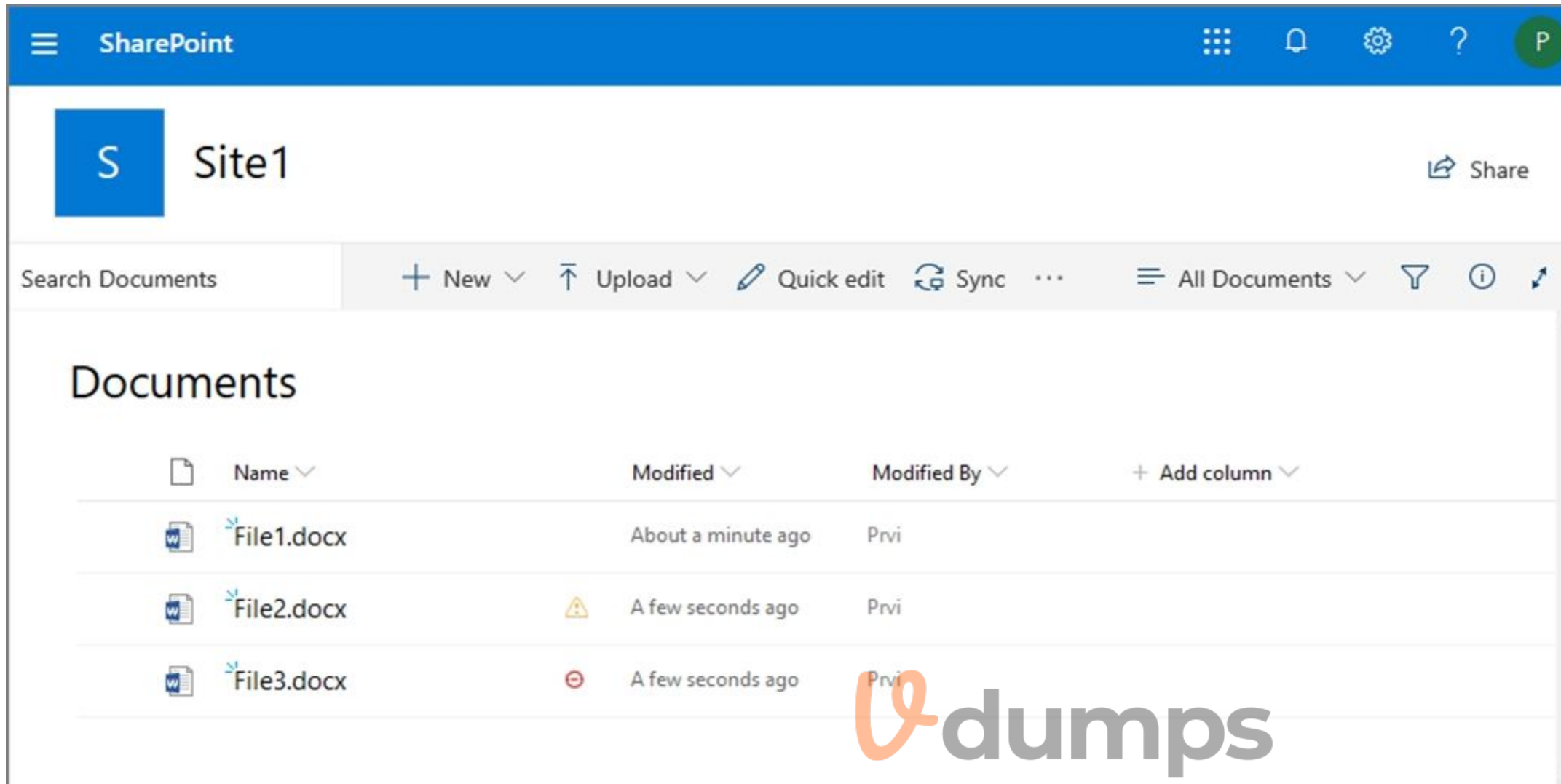
HOTSPOT

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.)





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.

Hot Area:

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

Answer Area:

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

Section:

Explanation:

<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/>
<https://gcc.microsoftcrmpartals.com/blogs/office365-news/190220SPIcons/>

QUESTION 62

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

Correct Answer: A, B, C

Section:

Explanation:

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

QUESTION 63

You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

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

Correct Answer: A

Section:

QUESTION 64

HOTSPOT

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.

Hot Area:



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

Answer Area:

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

QUESTION 65

HOTSPOT

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.

Hot Area:



Statements

Yes No

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

The SP800 assessment score will increase by 54 points.

The Data Protection Baseline score will increase by 9 points.

Answer Area:

Statements

Yes No

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

The SP800 assessment score will increase by 54 points.

The Data Protection Baseline score will increase by 9 points.

Section:

Explanation:

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

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#action-types-and-points>

QUESTION 66

You have a Microsoft 365 tenant.

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

Require complex passwords.

Require the encryption of data storage devices.

Have Microsoft Defender Antivirus real-time protection enabled.

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: B, D

Section:

Explanation:

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

**QUESTION 67**

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

- A. a retention policy
- B. a retention label policy
- C. an auto-labeling policy
- D. an insider risk policy

Correct Answer: C

Section:

Explanation:

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

QUESTION 68

DRAG DROP

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

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

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

Select and Place:

Actions

- Create a sensitivity label.
- Create an auto-labeling policy.
- Create a sensitive information type.
- Wait 24 hours, and then turn on the policy.
- Publish the label.
- Create a retention label.
- Wait eight hours, and then turn on the policy.

Answer Area

Empty answer area for the first question.

Correct Answer:**Actions**

- Empty action box
- Empty action box
- Empty action box
- Create a sensitive information type.
- Wait 24 hours, and then turn on the policy.
- Empty action box
- Empty action box
- Create a retention label.
- Wait eight hours, and then turn on the policy.

Answer Area

- Create a sensitivity label.
- Publish the label.
- Create an auto-labeling policy.

**Section:****Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-label-policies-can-do>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

QUESTION 69**HOTSPOT**

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

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

The tenant contains the devices shown in the following table.

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

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

Hot Area:

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

Answer Area:

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



Section:

Explanation:

QUESTION 70

DRAG DROP

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

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

You plan to join the devices to Azure Active Directory (Azure AD)

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, 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.

Select and Place:

Actions

- Disable BitLocker.
- Disable TPM.
- Switch to UEFI.
- Upgrade to Windows 10 Enterprise.

Answer Area

- Device1: Action
- Device2: Action
- Device3: Action

Correct Answer:

Actions

- Disable TPM.

Answer Area

- Device1: Disable BitLocker.
- Device2: Switch to UEFI.
- Device3: Upgrade to Windows 10 Enterprise.

Section:

Explanation:

QUESTION 71

HOTSPOT

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

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

You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD) Password hash synchronization is disabled.

You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure Azure AD Connect:

- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

To configure the domain:

- Add an alternative UPN suffix.
- Register a service connection point.
- Register a service principal name (SPN).

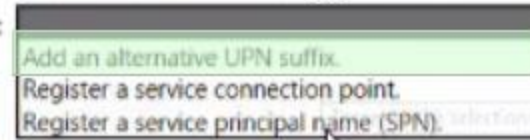
Answer Area:

Answer Area

To configure Azure AD Connect:



To configure the domain:



Section:

Explanation:

QUESTION 72

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices. You enable device clean-up rules. What can you configure as the minimum number of days before a device is removed automatically?

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

Correct Answer: D

Section:

QUESTION 73

You have a Microsoft 365 E5 subscription. You define a retention label that has the following settings:
* Retention period 7 years
* Start the retention period based on: When items were created
You need to prevent the removal of the label once the label is applied to a file. What should you select in the retention label settings?

- A. Retain items even if users delete
- B. Mark items as a record
- C. Mark items as a regulatory record
- D. Retain items forever

Correct Answer: B

Section:

QUESTION 74

HOTSPOT
You have several devices enrolled in Microsoft Endpoint Manager. You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.



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

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

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

You add user as a device enrollment manager in Endpoint manager

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

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 75

HOTSPOT

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

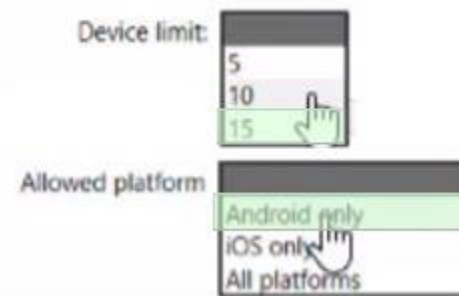
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:

Explanation:

QUESTION 76

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

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

Correct Answer: B

Section:

QUESTION 77

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription. You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center. Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1. Does this meet the goal?

- A. Yes
- B. No



Correct Answer: A

Section:

QUESTION 78

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

Correct Answer: A

Section:

QUESTION 79

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 User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 80

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 User4 to modify the Defender for identity sensor configuration.
Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 81

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profile?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

Correct Answer: B

Section:

Explanation:

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

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

Windows 10

macOS

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

Android Enterprise

Windows 8.1

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

QUESTION 82

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

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

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

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.

Does this meet the goal?

- A. Yes



B. No

Correct Answer: B

Section:

Explanation:

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

QUESTION 83

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

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

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

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

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

QUESTION 84

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

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

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

You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

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

QUESTION 85

HOTSPOT

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

You need to identify the following:

How many days it will take to establish a baseline for unusual activity.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

How many days it will take to establish the baseline:

1
5
7
10

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

Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

Answer Area:

How many days it will take to establish the baseline:

1
5
7
10

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

Alerts will be triggered.
Alerts will not be triggered.
Alerts will be triggered only after the process to establish the baseline has been running for one day.

Section:

Explanation:

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

QUESTION 86

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

Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

Correct Answer: B

Section:

Explanation:

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

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

QUESTION 87

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

You need to assign the Security Administrator role.

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

QUESTION 88

You have a Microsoft 365 E5 subscription.

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

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

What should you do first?

- A. Configure custom detection rules.

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 89

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.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 90

HOTSPOT

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

You need to configure Intune to meet the following requirements:

Prevent users from enrolling personal devices.

Ensure that users can enroll a maximum of 10 devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Prevent users from enrolling personal devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Answer Area:

Prevent users from enrolling personal devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions



Section:

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-windows-devices>

QUESTION 91

HOTSPOT

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

Name: Case1

Included content: Group1, User1, Site1

Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders

The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Holds are turned off for:

▼
User1 only
All locations
Site1 and Group1 only

Holds are placed on a delay hold for:

▼
30 days
90 days
120 days

Answer Area:

Holds are turned off for:

▼
User1 only
All locations
Site1 and Group1 only

Holds are placed on a delay hold for:

▼
30 days
90 days
120 days

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide>

QUESTION 92

HOTSPOT

You have a Microsoft 365 E5 tenant

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Choose locations to apply the policy

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

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

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

Answer Area:



Choose locations to apply the policy

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

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

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

Section:

Explanation:

QUESTION 93

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 [Close]

[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

Correct Answer: D

Section:

QUESTION 94

HOTSPOT

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

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

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

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

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

 Vdumps

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 95

HOTSPOT

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

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

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

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

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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

Hot Area:

Answer Area

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



Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 96

You have a Microsoft 365 E5 subscription.

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

You need to configure Microsoft Defender for Endpoint on the computers.

What should you create from the Endpoint Management admin center?

- A. a Microsoft Defender for Endpoint baseline profile

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

Correct Answer: D

Section:

QUESTION 97

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

- * Windows 10
- * Android
- * OS

On which devices can you configure the Endpoint DLP policies?

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

Correct Answer: C

Section:

Explanation:

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

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

QUESTION 98

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1, Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).

You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

- A. Windows 11 and Windows 10 only
- B. Windows 11, Windows 10, Windows 8.1, and macOS
- C. Windows 11 and macOS only
- D. Windows 11 only
- E. Windows 11, Windows 10, and Windows 8.1 only

Correct Answer: C

Section:

QUESTION 99

HOTSPOT

You have a Microsoft 365 E5 subscription that.

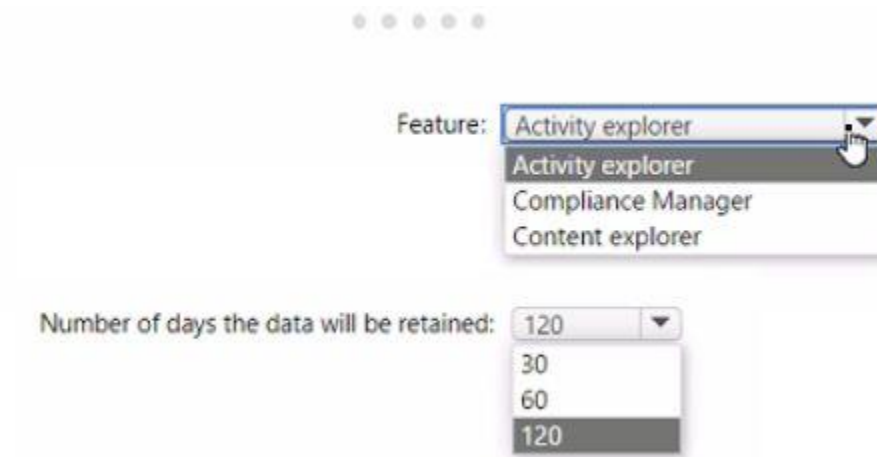
You need to identify whenever a sensitivity label is applied, changed, or removed within the subscription.

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

NOTE Each correct selection is worth one point.

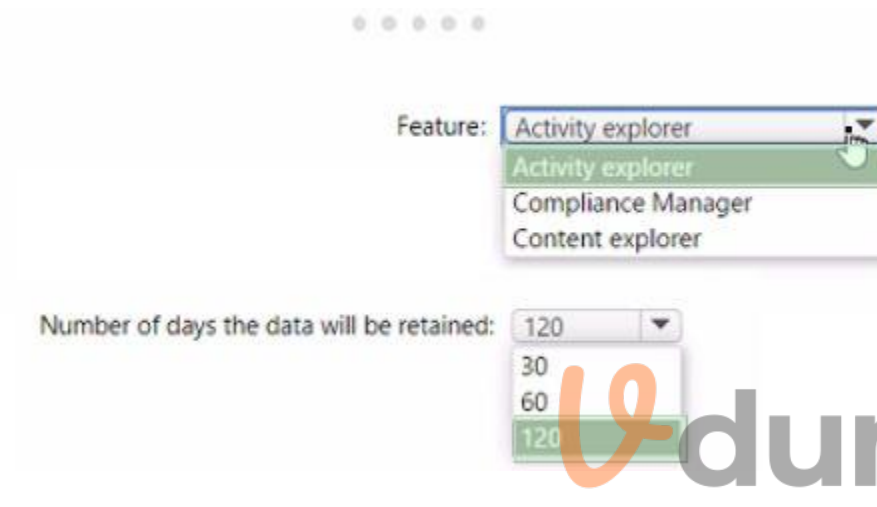
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:

Explanation:

QUESTION 100

Your network contains an Active Directory forest named contoso.local.

You purchase a Microsoft 365 subscription.

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

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

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

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

Correct Answer: D

Section:

Explanation:

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

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

Incorrect:

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

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

QUESTION 101

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

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

Correct Answer: C

Section:

Explanation:

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

Note: You can add the following types of groups:

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

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

Note:

Security groups

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

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

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

Security groups can be added to a team.

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

Microsoft 365 Groups

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

<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps>

<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?>

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>

QUESTION 102

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

- A. Enable auditing.
- B. Enable Microsoft 365 usage analytics.
- C. Create an Insider risk management policy.
- D. Create a communication compliance policy.

Correct Answer: A

Section:

Explanation:

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

QUESTION 103

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.

Correct Answer: B

Section:

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.

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



QUESTION 104

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

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

You need to remove User1 from the Restricted entities list.

What should you use?

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

Correct Answer: D

Section:

Explanation:

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

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam>

QUESTION 105

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do?

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

Correct Answer: D

Section:

Explanation:

Use the Microsoft 365 Defender portal to create Safe Links policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinks2>.

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

2. On the Name your policy page, configure the following settings:

Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

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

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

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

*-> Groups:

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

The specified Microsoft 365 Groups.

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

Etc.

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

QUESTION 106

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

Correct Answer: C

Section:

QUESTION 107

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?

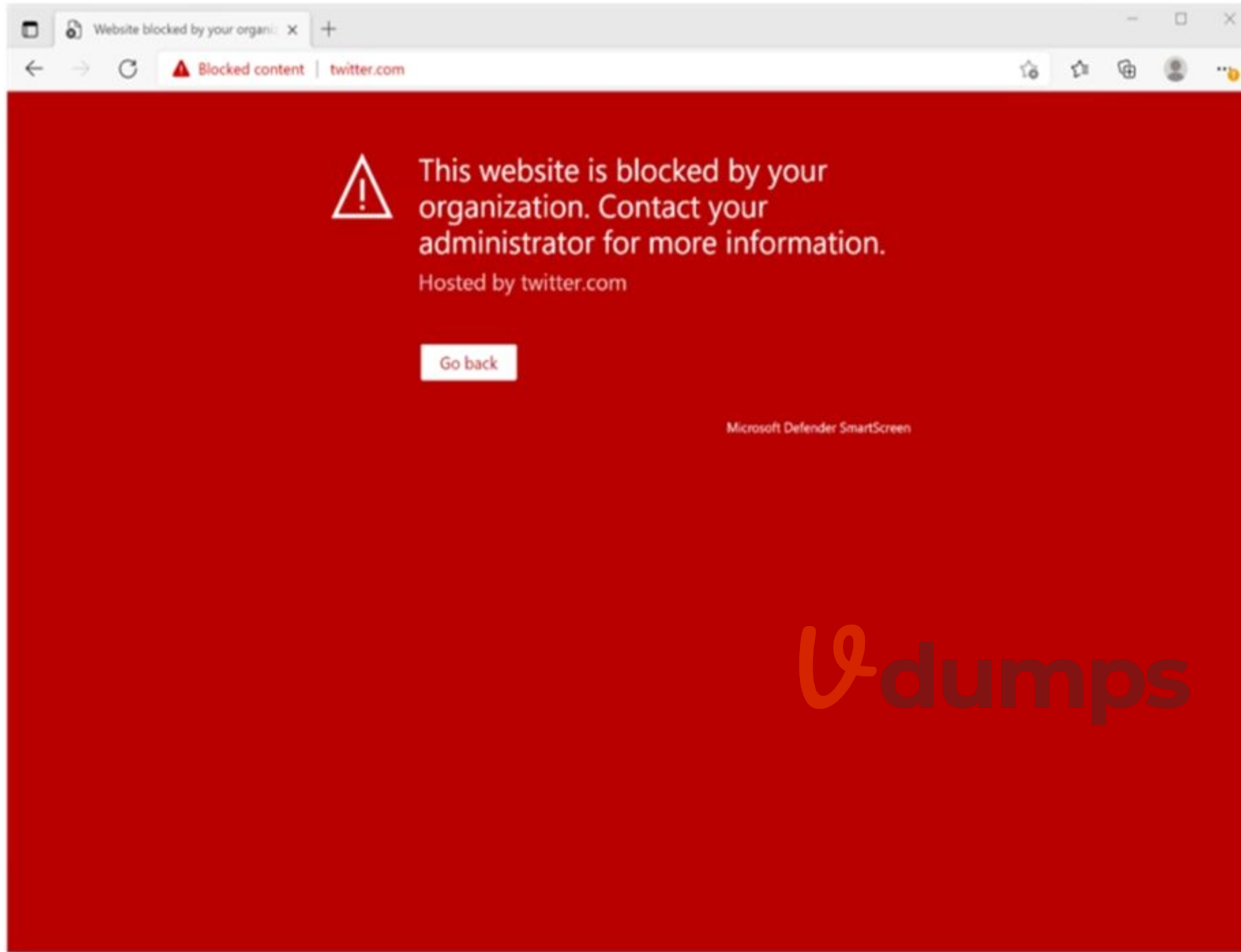
- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

Correct Answer: E

Section:

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.
<https://jadexstrategic.com/web-protection/>

QUESTION 108

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.

Hot Area:

Answer Area

Social engineering technique:

Credential harvest
Link to malware
Malware attachment

Training experience:

Identity Theft
Mass Market Phishing
Web Phishing

Answer Area:

Answer Area

Social engineering technique:

Credential harvest
Link to malware
Malware attachment

Training experience:

Identity Theft
Mass Market Phishing
Web Phishing

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started>

QUESTION 109

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

You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

What should you do?

- A. Create a new Anti-malware policy
- B. Configure the Safe Links global settings.
- C. Create a new Anti-phishing policy
- D. Configure the Safe Attachments global settings.

Correct Answer: D

Section:

Explanation:

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about>

QUESTION 110

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

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

You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully.

You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible.

What should you do?

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

Correct Answer: B

Section:

Explanation:

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

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

QUESTION 111

HOTSPOT

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

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

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

Settings > Endpoints > computer1



computer1

Device summary

Risk level ⓘ

None

Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

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

Hot Area:



Answer Area

Computer1 will be a member of [answer choice].

Group3 only
Group4 only
Group3 and Group4 only
Ungrouped devices

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

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

Answer Area:

Answer Area

Computer1 will be a member of [answer choice].

Group3 only
Group4 only
Group3 and Group4 only
Ungrouped devices

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

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

Section:

Explanation:

QUESTION 112

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 Directory, 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.

Correct Answer: A, B, E

Section:

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.

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

QUESTION 113

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.

Hot Area:

Answer Area

MFA method:

Call to phone
Email message
Security questions
Text message to phone
Notification to Microsoft Authenticator app

Number of days:

7
14
30
60

Answer Area:

Answer Area

MFA method:

Call to phone
Email message
Security questions
Text message to phone
Notification to Microsoft Authenticator app

Number of days:

7
14
30
60

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in>

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

QUESTION 114

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

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

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

Which objects will sync to Azure AD?

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

Correct Answer: D

Section:

Explanation:

Disabled accounts

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

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

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

QUESTION 115

You have a Microsoft 365 E5 subscription.

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

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

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

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

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

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

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

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

Correct Answer: B

Section:

Explanation:

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

One Policy.

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

One Policy.

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

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

One policy

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

Only users in the R&D department must be blocked from signing in from both Android

One Policy

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

QUESTION 116

HOTSPOT

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Tool:

<input type="checkbox"/>	AccessChk
<input type="checkbox"/>	Azure AD Connect
<input type="checkbox"/>	Active Directory Explorer
<input type="checkbox"/>	IdFix

Required group membership:

<input type="checkbox"/>	Domain Admins
<input type="checkbox"/>	Domain Users
<input type="checkbox"/>	Server Operators
<input type="checkbox"/>	Enterprise Admins

Answer Area:

Answer Area

Tool:

- AccessChk
- Azure AD Connect
- Active Directory Explorer
- IdFix

Required group membership:

- Domain Admins
- Domain Users
- Server Operators
- Enterprise Admins

Section:

Explanation:

<https://microsoft.github.io/idfix/>

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>



QUESTION 117

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.

Hot Area:

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"/>

Answer Area:

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 checked="" 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 checked="" type="checkbox"/>

Section:

Explanation:

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

QUESTION 118

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 Modem 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.

Correct Answer: A

Section:

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.

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

QUESTION 119

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

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

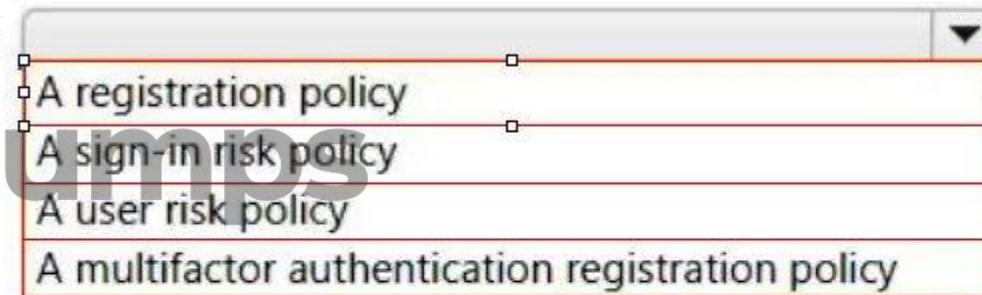
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

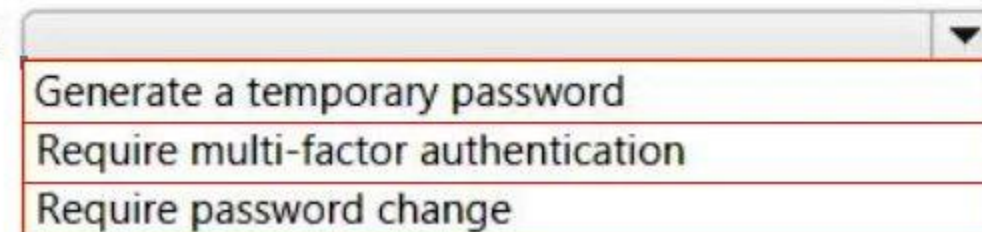
To identify when users have compromised credentials, configure:



A screenshot of a hot spot question interface. The question text is "To identify when users have compromised credentials, configure:". Below the text is a list of four options, each with a small square selection box to its left. The options are: "A registration policy", "A sign-in risk policy", "A user risk policy", and "A multifactor authentication registration policy". A large orange watermark "Vdumps" is overlaid on the list.

- A registration policy
- A sign-in risk policy
- A user risk policy
- A multifactor authentication registration policy

To enable self-remediation, select:



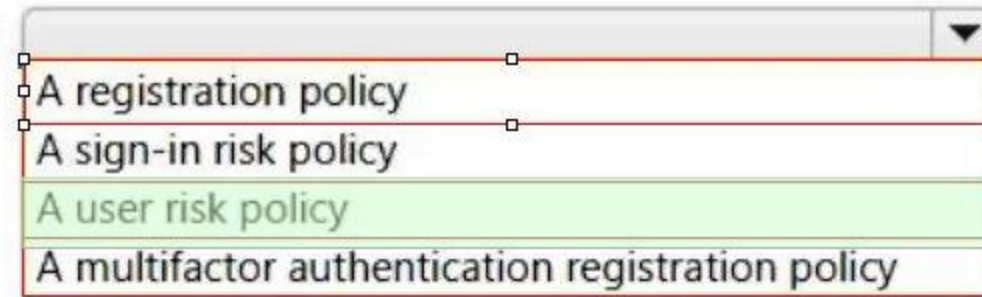
A screenshot of a hot spot question interface. The question text is "To enable self-remediation, select:". Below the text is a list of three options, each with a small square selection box to its left. The options are: "Generate a temporary password", "Require multi-factor authentication", and "Require password change".

- Generate a temporary password
- Require multi-factor authentication
- Require password change

Answer Area:

Answer Area

To identify when users have compromised credentials, configure:



A registration policy
A sign-in risk policy
A user risk policy
A multifactor authentication registration policy

To enable self-remediation, select:



Generate a temporary password
Require multi-factor authentication
Require password change

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#user-risk-based-conditional-access-policy>

QUESTION 120

HOTSPOT

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

The domain contains the users shown in the following table.

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

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

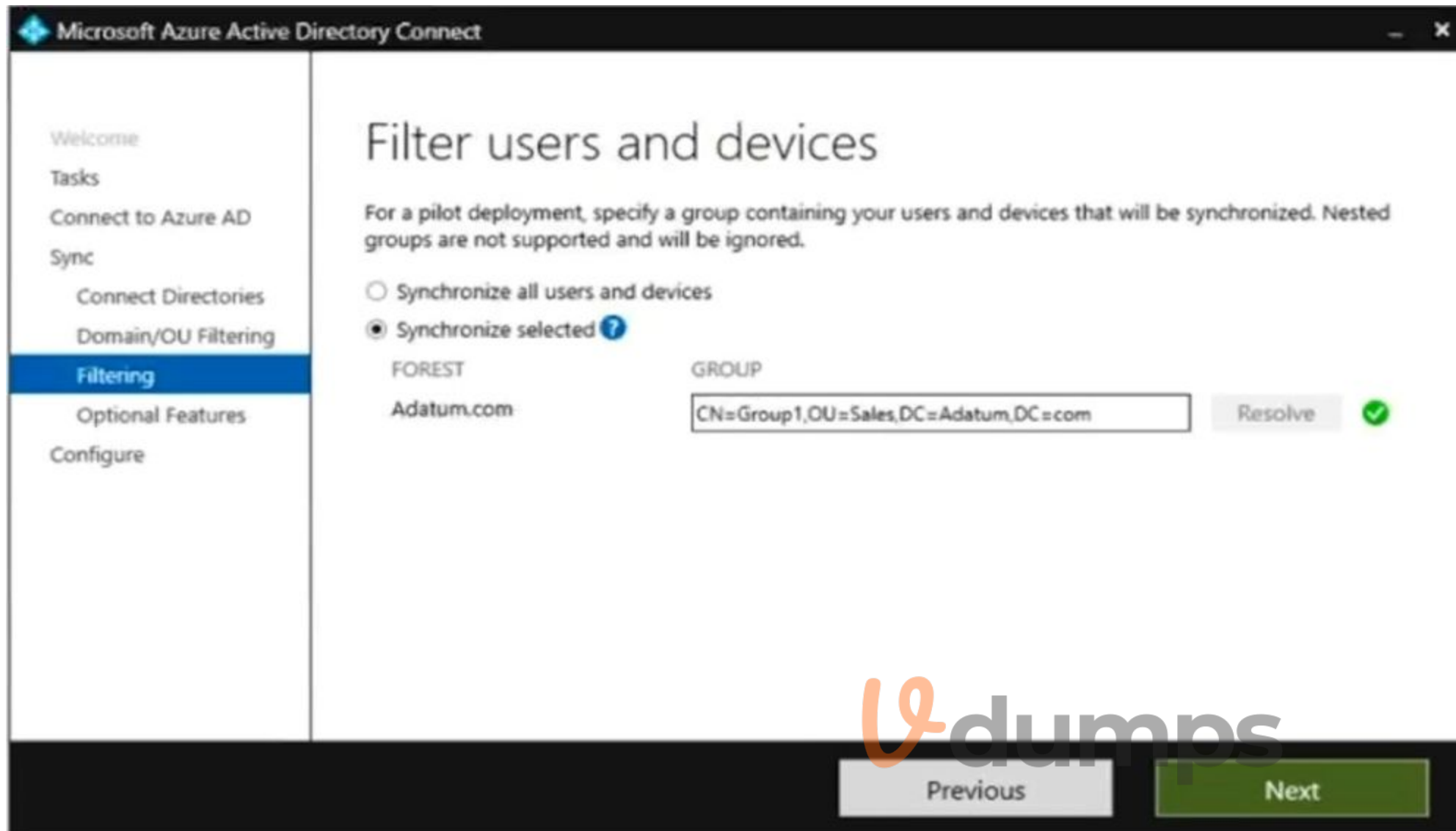
You are deploying Azure AD Connect.

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

Vdumps

The screenshot shows the 'Domain and OU filtering' configuration page in Microsoft Azure Active Directory Connect. The left sidebar contains navigation options: Welcome, Tasks, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering (highlighted), Filtering, Optional Features, and Configure. The main content area is titled 'Domain and OU filtering' and includes a note: 'If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.' Below this, the 'Directory' is set to 'Adatum.com' with a 'Refresh Domains' button. Two radio buttons are present: 'Sync all domains and OUs' (unselected) and 'Sync selected domains and OUs' (selected). A tree view shows the directory structure for 'Adatum.com' with the following items and their selection status: Builtin (unchecked), Computers (unchecked), Development (unchecked), Domain Controllers (unchecked), ForeignSecurityPrincipals (unchecked), Infrastructure (unchecked), IT (unchecked), LostAndFound (unchecked), Managed Service Accounts (unchecked), Managers (unchecked), Marketing (unchecked), OU1 (checked), Program Data (unchecked), Sales (unchecked), System (unchecked), and Users (unchecked). At the bottom, there are 'Previous' and 'Next' buttons.

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



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

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 121

HOTSPOT

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

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	None

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Any

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.

User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.

User3 can use passwordless authentication without further action.

Yes

No

Answer Area:

Answer Area

Statements

User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.

User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.

User3 can use passwordless authentication without further action.

Yes

No

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone>

QUESTION 122

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)	<i>Not applicable</i>

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.

Hot Area:

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.

Answer Area:

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.

Section:

Explanation:

QUESTION 123

HOTSPOT

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

Contoso.com

East.contoso.com

The forest contains the users shown in the following table.

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

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

Vdumps

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

vdumps

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

Hot Area:

Answer Area

Statements

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

User1 can authenticate to Azure AD by using a username of user1@contoso.com.

User2 can authenticate to Azure AD by using a username of user2@contoso.com.

User3 can authenticate to Azure AD by using a username of user3@contoso.com.

Answer Area:

Answer Area

Statements

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

User1 can authenticate to Azure AD by using a username of user1@contoso.com.

User2 can authenticate to Azure AD by using a username of user2@contoso.com.

User3 can authenticate to Azure AD by using a username of user3@contoso.com.

Section:

Explanation:

QUESTION 124

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.

Hot Area:

Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Answer Area:

Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

 Vdumps

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install>

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites>

QUESTION 125

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.

Hot Area:

Answer Area



Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Answer Area:

Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install>

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites>

QUESTION 126

You have a Microsoft 365 subscription.

You add a domain named contoso.com. When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com. You need to change the email address used to verify the domain. What should you do?

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

Correct Answer: C

Section:

QUESTION 127

DRAG DROP

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.

All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.

You plan to implement self-service password reset (SSPR).

You need to ensure that when a user resets or changes a password, the password syncs with AD DS.

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or



scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Actions

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

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

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

Step 2:

Step 3:



Correct Answer:

Actions

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Answer Area

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

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

Step 3: Select Password writeback in Microsoft Entra Connect.

Section:

Explanation:

QUESTION 128

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

You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.

What should you use?

- A. Microsoft Secure Score
- B. Cloud discovery
- C. Exposure distribution
- D. Threat tracker
- E. Exposure score

Correct Answer: A

Section:

QUESTION 129

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

Correct Answer: B
Section:

