

Microsoft.MS-102.vJul-2024.by.Aney.209q

Number: MS-102
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: MS-102

Exam Name: Microsoft 365 Administrator



Case A

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

HOTSPOT

Overview

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

Environment

On-Premises Environment

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Cloud Environment

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

Problem Statements

Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements

Planned Changes

Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements

Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
 - Join Microsoft Teams channels.
 - Join Microsoft Teams chats.
 - Access shared files.
- Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.



- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

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 2

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: B

Section:

Explanation:

Security Reader

View and investigate active threats to your Microsoft 365 users, devices, and content.

QUESTION 3

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

dumps

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 4

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 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

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

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: C

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide#add-a-domain>

QUESTION 8

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 9

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 10

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:

Case B

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 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 2

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>

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 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 5

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 6

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 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: ▼

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 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

Policy type: 


- Label
- Retention**
- Auto-labeling

Number of required policies: 


- 1
- 2**
- 3

Answer Area:

Answer Area

Policy type: 

- Label
- Retention**
- Auto-labeling

Number of required policies: 

- 1
- 2**
- 3

Section:

Explanation:

Case C

Case Study:

Overview

Existing Environment

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included 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.

When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure

A. Datum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements

Requirements

A. Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Business Goals

A. Datum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A. Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A. Datum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive US.

PII data to other New York office users. Email messages must be monitored to ensure compliance.

Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION 1

HOTSPOT

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

Hot Area:

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

<input type="checkbox"/>	Audit log
<input type="checkbox"/>	Data governance events
<input type="checkbox"/>	DLP policy matches
<input type="checkbox"/>	eDiscovery

Filter by:

<input type="checkbox"/>	Activity
<input type="checkbox"/>	Detail
<input type="checkbox"/>	Item
<input type="checkbox"/>	User agent

Answer Area:

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

▼
Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by:

▼
Activity
Detail
Item
User agent

Section:

Explanation:

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

QUESTION 2

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

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



Correct Answer: B

Section:

Explanation:

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

QUESTION 3

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

Correct Answer: A

Section:

Explanation:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage

your time to ensure that you are able to complete all questions included 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.

QUESTION 4

You need to meet the technical requirement for the EU PII data.

What should you create?

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

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 5

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

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



Correct Answer: D

Section:

Explanation:

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

QUESTION 6

DRAG DROP

You need to meet the requirement for the legal department.

Which three actions should you perform in sequence from the Security & Compliance admin center? 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 data loss prevention (DLP) policy.
- Create an eDiscovery case.
- Create a label.
- Run a content search.
- Create a label policy.
- Create a hold.
- Assign eDiscovery permissions.
- Publish a label.

Answer Area

Correct Answer:

Actions

- Create a data loss prevention (DLP) policy.
-
- Create a label.
- Run a content search.
- Create a label policy.
-
-
- Publish a label.

Answer Area

Assign eDiscovery permissions.
Create an eDiscovery case.
Create a hold.



Section:

Explanation:

<https://www.sherweb.com/blog/ediscovery-office-365/>

QUESTION 7

HOTSPOT

You need to meet the technical requirement for log analysis.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Minimum number of data sources:

Minimum number of log collectors:

Answer Area:

Minimum number of data sources:

Minimum number of log collectors:



Section:

Explanation:

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

QUESTION 8

Which report should the New York office auditors view?

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

Correct Answer: C

Section:

Explanation:

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

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

Exam D

QUESTION 1

HOTSPOT

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

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

* The number of email messages quarantined by zero-hour auto purge (ZAP)

* The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection



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

Mailflow status report ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

Answer Area:



Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

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

Mailflow status report ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

Section:

Explanation:

QUESTION 2

HOTSPOT

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



Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1: ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Answer Area:
Answer Area

Device1: ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Section:
Explanation:

QUESTION 3

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

Labels Label policies Auto-labeling (preview)

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

+ Create a label Publish labels Refresh

Name ↑		Order	Created by	Last modified
Label1	...	0 - highest	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. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label2, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

Correct Answer: C

Section:

QUESTION 4

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

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

What should you do first?

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

Correct Answer: D

Section:

QUESTION 5

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

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

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings.

Which devices will support the settings?

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



Correct Answer: A

Section:

QUESTION 6

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

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

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

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

Correct Answer: A

Section:

QUESTION 7

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

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

What should you do on the computer?

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

Correct Answer: C

Section:

QUESTION 8

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

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

Correct Answer: C

Section:

**QUESTION 9**

DRAG DROP

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

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

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Policy Types

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

Answer Area

Device1:

Device2:

Device3:

Correct Answer:

Policy Types

- App configuration policy
-
-
-

Answer Area

Device1: App protection policy

Device2: Conditional Access policy

Device3: Compliance policy



Section:

Explanation:

QUESTION 10

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

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

Correct Answer: D

Section:

QUESTION 11

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



Feature:

- Activity explorer
- Activity explorer
- Compliance Manager
- Content explorer

Number of days the data will be retained:

- 30
- 60
- 120

Answer Area:

Answer Area



Feature:

- Activity explorer
- Activity explorer
- Compliance Manager
- Content explorer

Number of days the data will be retained:

- 30
- 60
- 120

Section:

Explanation:

QUESTION 12

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 ⓘ Allow Block

Send org data to other apps ⓘ Policy managed apps

Select apps to exempt

Save copies of org data ⓘ Allow 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 ⓘ Allow 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 ⓘ Allow Block

Approved keyboards ⓘ Require Not required

Select keyboards to approve

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

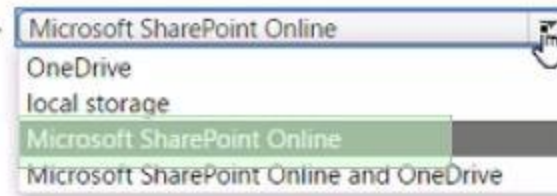
A user can copy and paste text from [answer choice] to a Microsoft Word document stored in Microsoft OneDrive.

- 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.



A dropdown menu with a downward arrow on the right. The menu is open, showing four options: "Microsoft SharePoint Online", "OneDrive", "local storage", and "Microsoft SharePoint Online and OneDrive". The "Microsoft SharePoint Online" option is highlighted with a green background.

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



A dropdown menu with a downward arrow on the right. The menu is open, showing three options: "any app", "only managed apps", and "only unmanaged apps". The "any app" option is highlighted with a green background.

Section:

Explanation:

QUESTION 13

HOTSPOT

Your company has a Microsoft 365 E5 tenant.

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

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

The company currently uses the following Office file types:

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

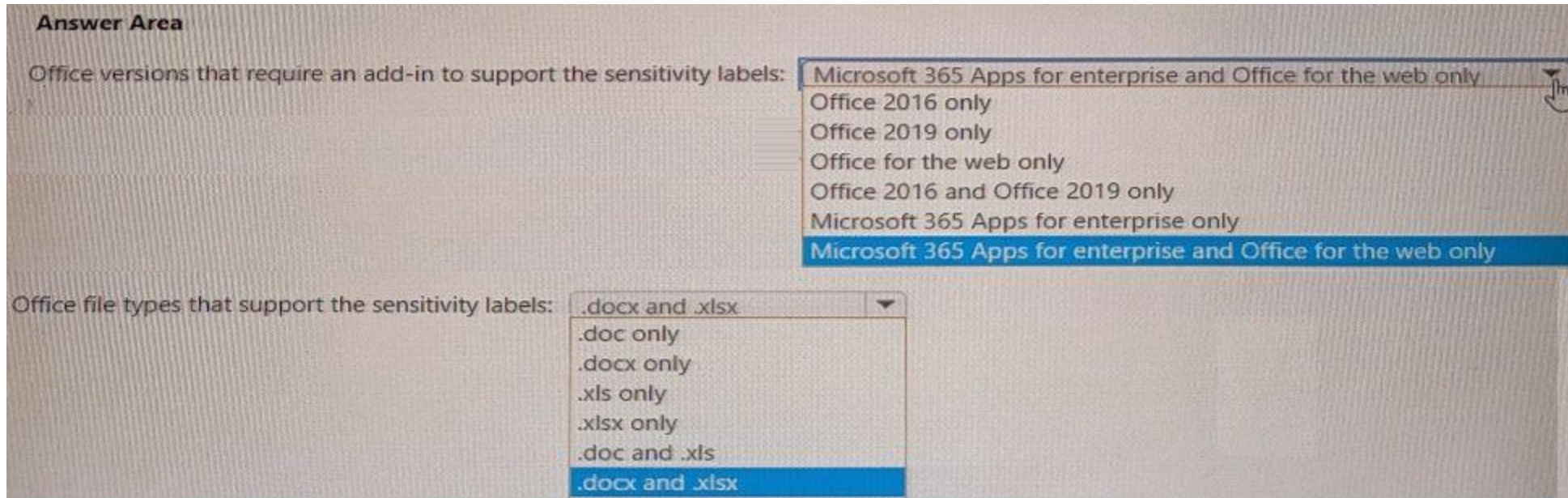
You plan to use sensitivity labels. You need to identify the following:

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

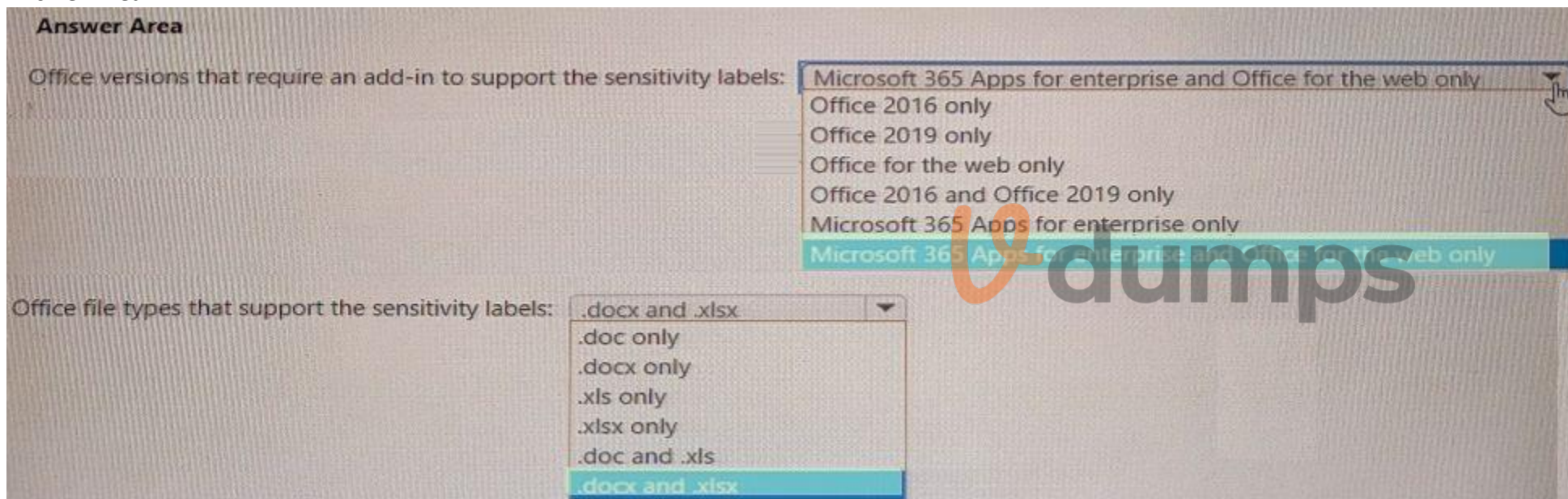
What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.

Hot Area:





Answer Area:



Section:

Explanation:

QUESTION 14

HOTSPOT

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

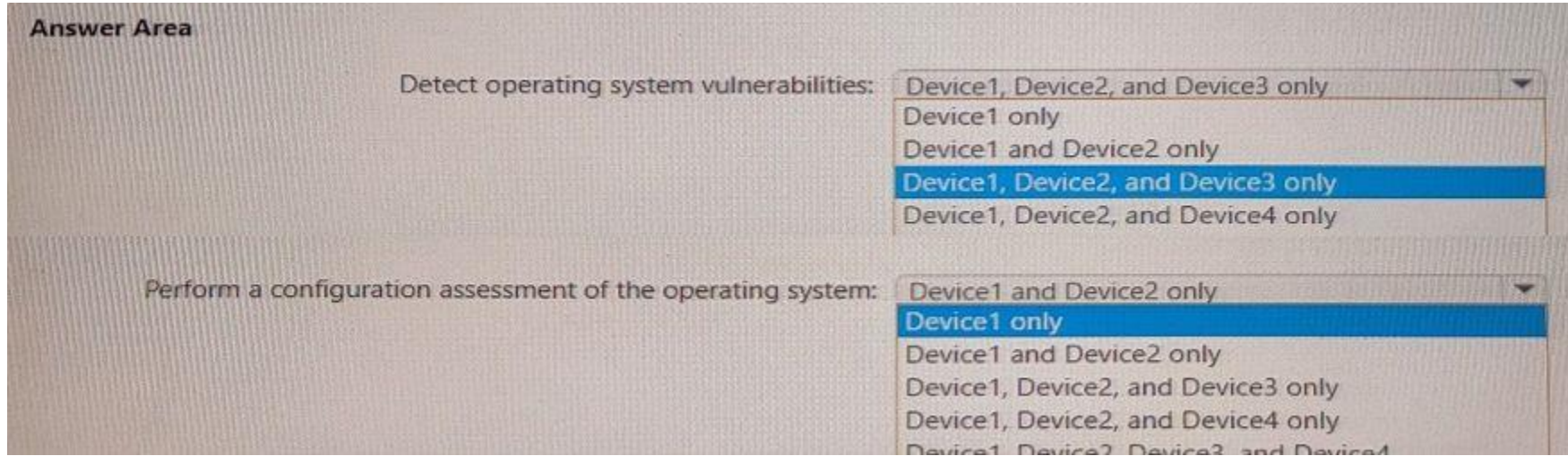
Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint

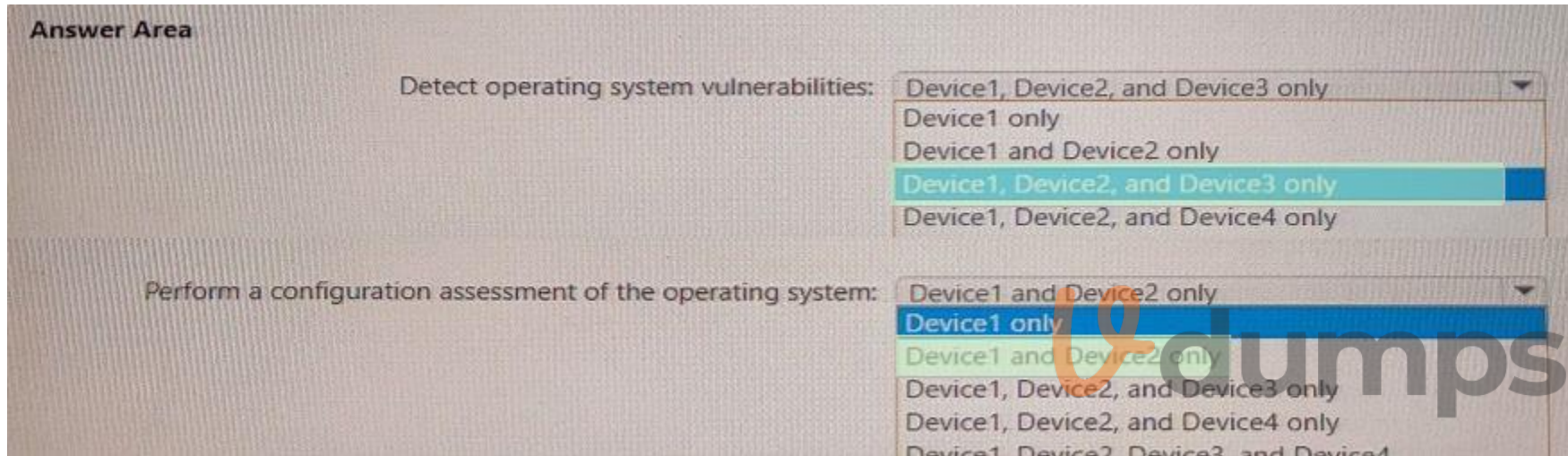
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

* Detect operating system vulnerabilities.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 15

HOTSPOT

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

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy ✕

Name *

Description

Record Types

Activities

Users:

Show results for all users

Duration *

90 Days

6 Months

1 Year

Priority *

You plan to create a new user named User1.

How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.

Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 16

You have a Microsoft 365 subscription.

From 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 Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

QUESTION 17

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

A Built-in protection preset security policy is applied to the subscription.

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

NOTE: Each correct selection is worth one point.

A. Anti-malware

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

Correct Answer: C, E
Section:

QUESTION 18
HOTSPOT

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

Hot Area:
Answer Area

Portal:

Feature:

Answer Area:
Answer Area

Portal:

Feature:

Section:
Explanation:

QUESTION 19

HOTSPOT

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

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Word is installed on Device1.

Yes

No

App3 is displayed in the Company Portal.

Excel is installed on Device1.

Answer Area:



Answer Area

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

Section:

Explanation:

QUESTION 20

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune.

Which platform can you manage by using the profiles?

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

Correct Answer: D

Section:

QUESTION 21

You have a Microsoft 365 E5 tenant.

Industry regulations require that the tenant comply with the ISO 27001 standard.

You need to evaluate the tenant based on the standard

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

Correct Answer: B

Section:

QUESTION 22

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.

You need to enable unified labeling for Microsoft 365 groups.

Which cmdlet should you run?

- A. set-unifiedGroup



- B. Set-Labelpolicy
- C. Execute-AzureAdLabelSync
- D. Add-UnifiedGroupLinks

Correct Answer: C

Section:

QUESTION 23

You have a Microsoft 365 E5 tenant.

You configure sensitivity labels.

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

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

What should you do?

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

Correct Answer: B

Section:

QUESTION 24

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

Captures Microsoft Teams channel messages that contain threatening or violent language.

Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

- A. Data Subject Requests (DSRs)
- B. Insider risk management policies
- C. Communication compliance policies
- D. Audit log retention policies

Correct Answer: C

Section:

QUESTION 25

Your company has a Microsoft 365 subscription.

you implement sensitivity Doris for your company.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

- A. a sharing policy from the Exchange admin center
- B. a mail flow rule from the Exchange admin center
- C. a message Dace from the Microsoft 365 security center
- D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center



Correct Answer: B

Section:

QUESTION 26

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You need to prevent the members of Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other users in the tenant. What should you use?

- A. information barriers
- B. communication compliance policies
- C. moderated distribution groups
- D. administrator units in Azure Active Directory (Azure AD)

Correct Answer: A

Section:

QUESTION 27

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

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

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

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

Correct Answer: D

Section:

QUESTION 28

HOTSPOT

You have device compliance policies shown in the following table.

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

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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 29

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft Intune.

You plan to use Endpoint analytics to identify hardware issues.

You need to enable Windows health monitoring on the devices to support Endpoint analytics.

What should you do?

- A. Configure the Endpoint analytics baseline regression threshold.
- B. Create a configuration profile.
- C. Create a Windows 10 Security Baseline profile.
- D. Create a compliance policy.

Correct Answer: B

Section:

QUESTION 30

HOTSPOT

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

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

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

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

Users may register their devices with Azure AD ⓘ

All None

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

Require Multi-Factor Auth to join devices ⓘ

Yes No

Maximum number of devices per user ⓘ

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 31

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. Android

- B. CentOS Linux
- C. iOS
- D. Window 10

Correct Answer: D

Section:

Explanation:

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

QUESTION 32

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

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

What should you do on the computer?

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

Correct Answer: B

Section:

QUESTION 33

HOTSPOT

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.



Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are shown in the following exhibit.

Microsoft Remote Desktop

Free • Online • [Product Details](#)

Install

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

Settings & Actions

Not in private store

[More actions available on details page](#)

Excel Mobile

Free • Online • [Product Details](#)

Install

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

Settings & Actions

In private store

[More actions available on details page](#)



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
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements

Yes

No

User2 can install the Microsoft Remote Desktop app from the private store.

User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.

User4 can manage the Microsoft Remote Desktop app from the private store.

Section:

Explanation:

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

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.

You have a computer that runs Windows 10.

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

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

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



QUESTION 35

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

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

Which properties of the alerts can you modify?

A. Status only

B. Status and Comment only

C. Status and Severity only

D. Status, Severity, and Comment only

E. Status, Severity, Comment and Category

Correct Answer: B

Section:

Explanation:

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

QUESTION 36

DRAG DROP

Your company purchases a cloud app named App1.

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

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

<https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security>

Select and Place:

Actions

Answer Area

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Cloud App Security admin center, add an app connector.

Sign in to App1.

Create a conditional access policy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for App1.



Correct Answer:

Actions

Deploy Azure Active Directory (Azure AD) Application Proxy.
From the Azure Active Directory admin center, configure the Diagnostic settings.
From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

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



Section:

Explanation:

<https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security>

QUESTION 37

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.

Devices are onboarded by using Microsoft Defender for Endpoint.

You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.

What should you create first?

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 38

HOTSPOT

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

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

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

Home / Policy Management 🔔 Notifications

Policy configurations

+ Create 📄 Copy ↕ Reorder priority 🗑️ Remove Total policy configurations: 3

Name	Priority ↑	Recommendation status
Office Users Policy	0	
Sales Team Policy	1	
All users	2	

The policies use the settings shown in the following table.

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hot Area:

The default shared folder location for User1 is:

▼

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

▼

Colorful

Dark Gray

White

Answer Area:

The default shared folder location for User1 is:

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

The default Office theme for User 2 is:

	▼
Colorful	
Dark Gray	
White	

Section:

Explanation:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

QUESTION 39

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint. From Microsoft Defender Security Center, you perform a security investigation. You need to run a PowerShell script on the device to collect forensic information. Which action should you select on the device page?

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 40

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

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

Correct Answer: B

Section:

Explanation:

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



QUESTION 41

HOTSPOT

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.



Hot Area:

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

Answer Area:

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

Section:

Explanation:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

QUESTION 42

You have a Microsoft 365 tenant.

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

What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

Correct Answer: D

Section:

Explanation:

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

QUESTION 43

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

You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.

Which policy type should you configure?

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



Correct Answer: A

Section:

Explanation:

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

QUESTION 44

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

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

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

- A. only the settings of Policy1
- B. only the settings of Policy2

- C. only the settings of Policy3
- D. no settings

Correct Answer: D

Section:

QUESTION 45

HOTSPOT

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
	lookup		
	project		
	render		
	where		



Answer Area:

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
	lookup		
	project		
	render		
	where		

Section:

Explanation:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968>

QUESTION 46

HOTSPOT

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Devices that can onboarded to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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



Answer Area:

Devices that can onboarded to Microsoft Defender for Endpoint:

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

Endpoint security policies that must be configured:

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

Section:

Explanation:

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

QUESTION 47

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

You plan to implement insider risk management.

You need to ensure that User1 can perform the following tasks:

Review alerts.

Manage cases.

Create notice templates.

Review user emails by using Content explorer.

The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Insider Risk Management
- B. Insider Risk Management Analysts
- C. Insider Risk Management Investigators
- D. Insider Risk Management Admin

Correct Answer: C

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide>

QUESTION 48

Your company has a Microsoft 365 E5 tenant that contains a user named User1.

You review the company's compliance score.

You need to assign the following improvement action to User1:Enable self-service password reset.

What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).



- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Correct Answer: D

Section:

Explanation:

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

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

QUESTION 49

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard.

You need to assess the company's current state of compliance.

What should you use?

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 50

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams

Microsoft OneDrive

Microsoft Exchange Online

Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 51

HOTSPOT

You have a Microsoft 365 E5 tenant.



You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)
You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)
A user sends an email that contains the components shown in the following table.
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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

Answer Area:

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



Section:

Explanation:

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

QUESTION 52

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

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

Correct Answer: B

Section:

Explanation:

QUESTION 53

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 54

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 55

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 56

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 57

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 58

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 59

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:	<input type="text"/>
	No profiles
	Profile1 only
	Profile4 only
	Profile1 and Profile4 only
	Profile1, Profile1, and Profile4 only
Device2:	<input type="text"/>
	No profiles
	Profile1 only
	Profile2 only
	Profile3 only
	Profile1 and Profile2 only
	Profile2 and Profile3 only



Answer Area:

Device 1:

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

Device 2:

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

Section:

Explanation:

QUESTION 60

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 61

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 62

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 63

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 64

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>

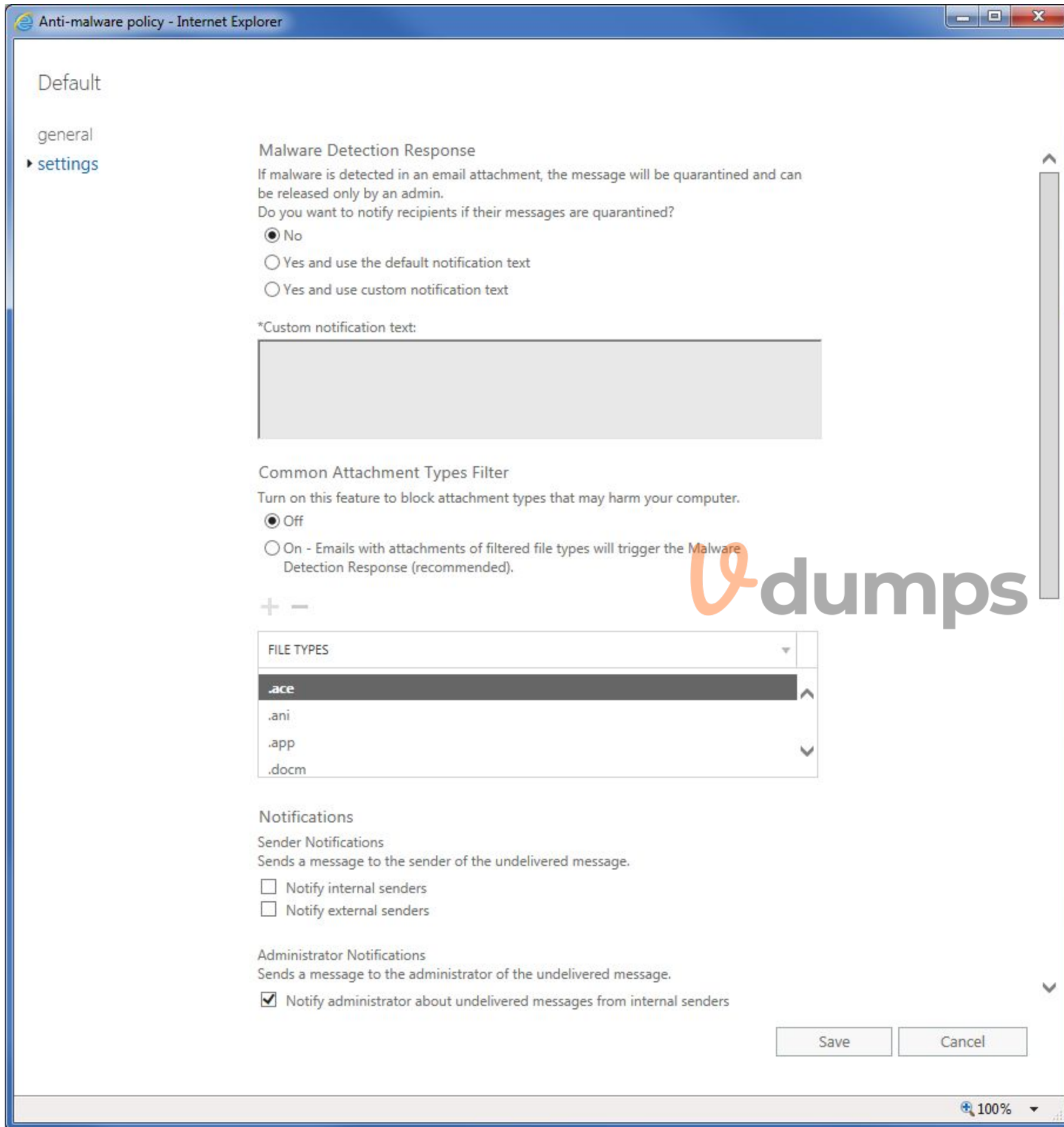
<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>



QUESTION 65

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

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



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

How will the email message and the attachments be processed?

- A. Both attachments will be 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 66

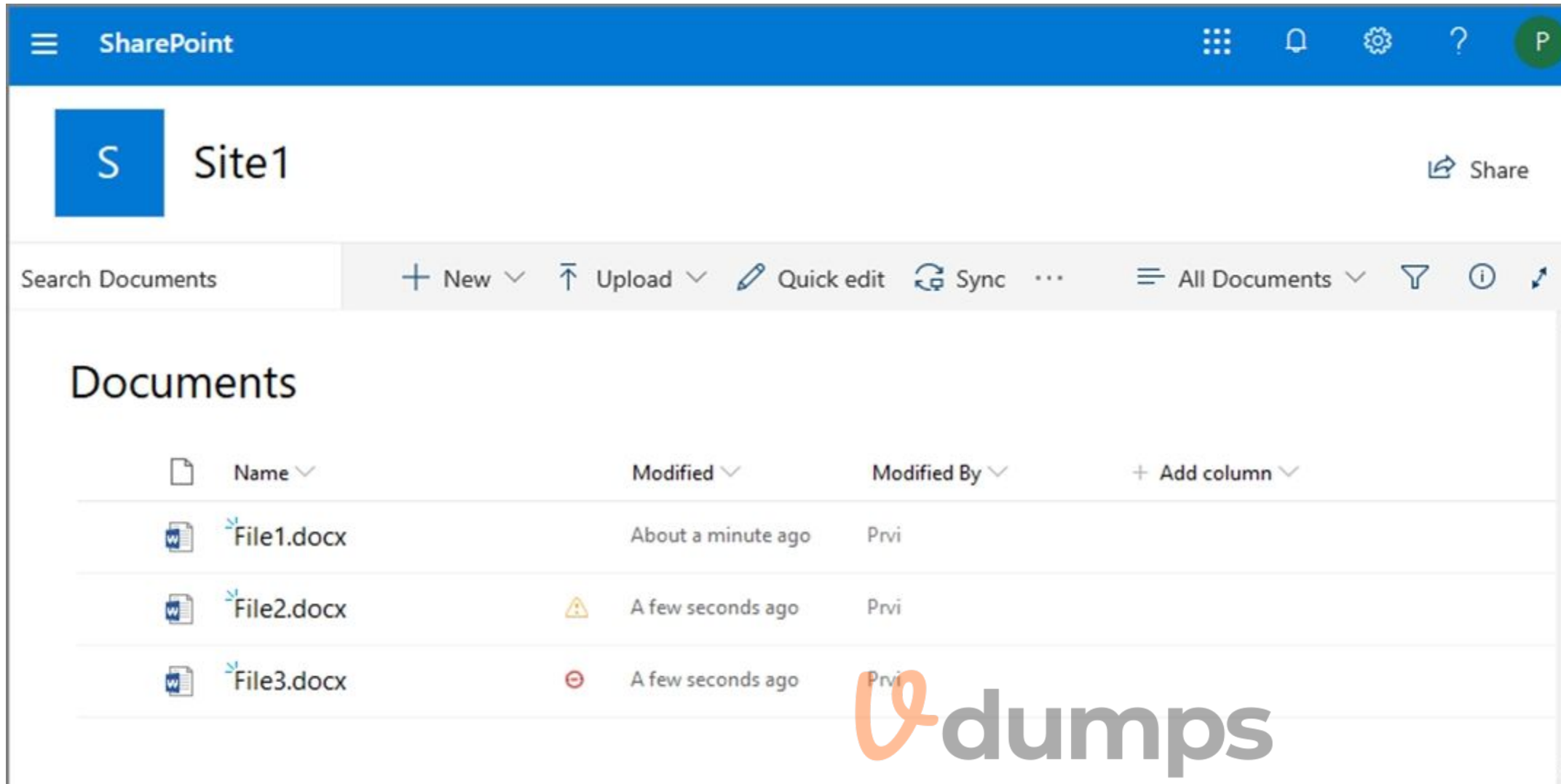
HOTSPOT

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 67

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 68

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 69

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 70

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 71

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 72**

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 73

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

Correct Answer:

Actions

Create a sensitive information type.

Wait 24 hours, and then turn on the policy.

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 74

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

You configure a session control policy to block downloads from SharePoint Online sites.

Users report that they can still download files from SharePoint Online sites.

You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.

What should you configure?

- A. an access policy
- B. a data loss prevention (DLP) policy
- C. an activity policy

D. a Conditional Access policy

Correct Answer: A

Section:

QUESTION 75

HOTSPOT

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

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

Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Rename:


- File1 only
- File1 and File2 only
- File1, File2, and File3 only**
- File1, File2, File3, and File4

Delete:


- File1 only
- File1 and File2 only**
- File1, File2, and File3 only
- File1, File2, File3, and File4

Answer Area:

Answer Area

Rename: 

- File1 only
- File1 and File2 only
- File1, File2, and File3 only**
- File1, File2, File3, and File4

Delete: 

- File1 only
- File1 and File2 only**
- File1, File2, and File3 only
- File1, File2, File3, and File4

Section:

Explanation:

QUESTION 76

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 77

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 78

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 79

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 80

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 81

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) and (user.department)

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

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

Answer Area:

Answer Area

(user.userType) and (user.department)

-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 82

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 83
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 84

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)

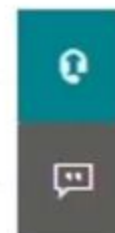
Issues in your environment that require action (0)



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 85

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 86

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 87

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 88

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 89

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 90

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 91

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 92

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/safelinksv2>.

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

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

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

Description: Enter an optional description for the policy.

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

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

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

*-> Groups:

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

The specified Microsoft 365 Groups.

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

Etc.

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



QUESTION 93

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 94

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 95

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 96

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)	<i>Not applicable</i>

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 97

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

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

Opening files in Microsoft SharePoint that contain malicious content

Impersonation and spoofing attacks in email messages

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Opening files in SharePoint that contain malicious content:

	▼
Anti-spam	
Anti-Phishing	
Safe Attachments	
Safe Links	

Impersonation and spoofing attacks in email messages:

	▼
Anti-spam	
Anti-Phishing	
Safe Attachments	
Safe Links	

Answer Area:

Answer Area

Opening files in SharePoint that contain malicious content:

	▼
Anti-spam	
Anti-Phishing	
Safe Attachments	
Safe Links	

Impersonation and spoofing attacks in email messages:

	▼
Anti-spam	
Anti-Phishing	
Safe Attachments	
Safe Links	

Section:

Explanation:

QUESTION 98

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.



This website is blocked by your organization. Contact your administrator for more information.

Hosted by www.contoso.com

Go back

Microsoft Defender SmartScreen

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

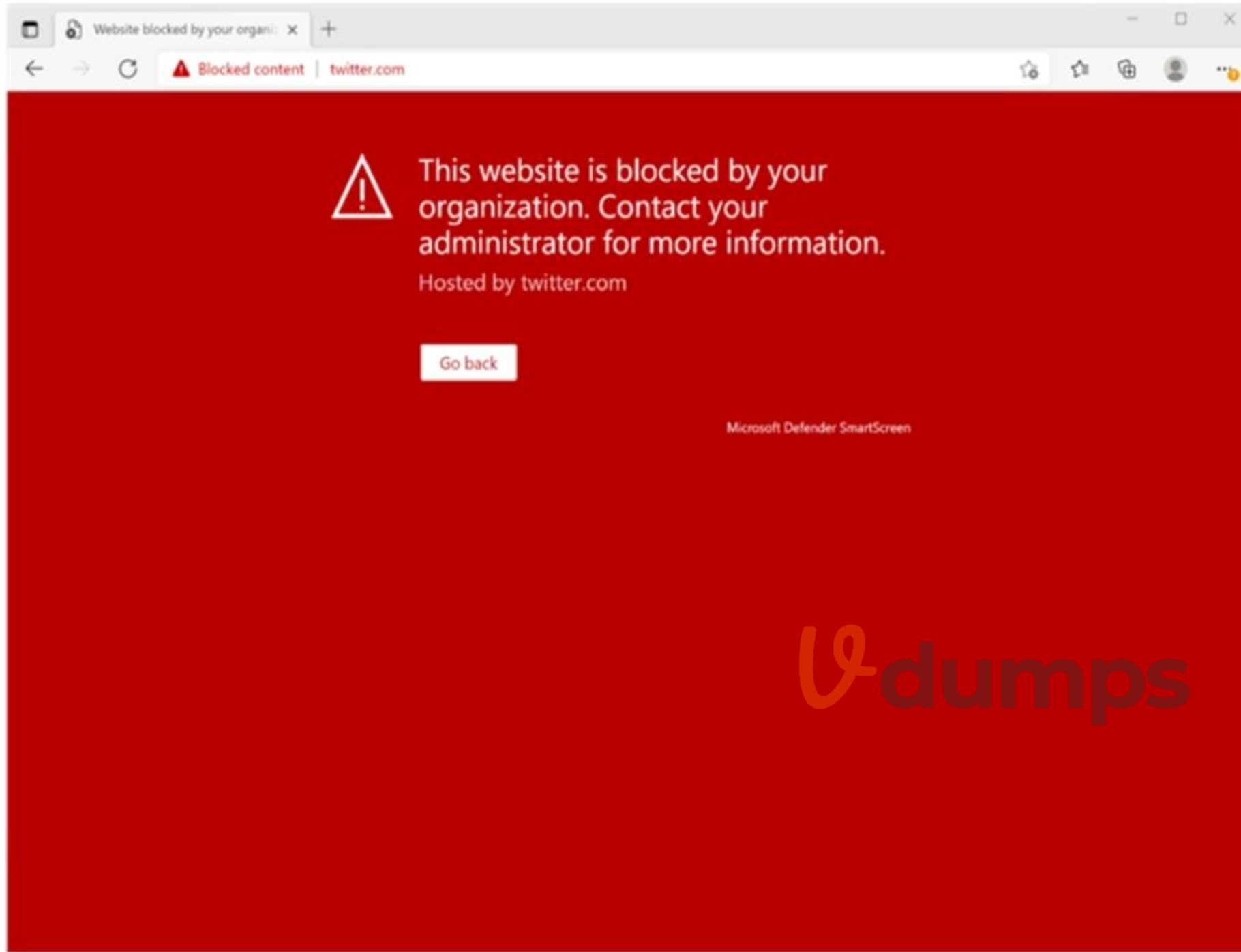
- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

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 99

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery

E. attack surface reduction (ASR)

Correct Answer: B, E

Section:

Explanation:

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting

The Microsoft 365 Defender portal (<https://security.microsoft.com>) provides easy access to information about detected threats and actions to address those threats.

The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created.

The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.

The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.

The Reports section includes reports that show threats detected and their status.

E: What can you expect from Microsoft Defender for Endpoint P1?

Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:

Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.

(E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.

Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.

The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

**Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1>

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan-1-now-included-in-m365-e3/ba-p/3060639>

QUESTION 100

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

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

Correct Answer: C

Section:

Explanation:

Data retention information for Microsoft Defender for Office 365

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

Defender for Office 365 Plan 1

* Alert metadata details (Microsoft Defender for Office alerts)

90 days.

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

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
Email reported by ...		Informational		In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Custom detection -...		Medium		New	Execution	Custom detection	msdo@sdf3p1.on...	Apr 14, 2021
"> <img src=x oner...	+5	High	No threats found	New	Exploit	Custom detection	cont-denamarks	Apr 14, 2021
"> <img src=x oner...	+2	High	No threats found	New	Exploit	Custom detection	cont-mikebarden	Apr 7, 2021
Unfamiliar sign-in ...		Low		New	Initial access	AAD Identity Protection	bbsecadmin	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Test email custom ...		Medium		New	Execution	Custom detection	Clare Love	Apr 14, 2021

QUESTION 101

You have a Microsoft 365 E5 subscription.

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

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

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

Correct Answer: C

Section:

Explanation:

View email security reports in the Microsoft 365 Defender portal

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

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

QUESTION 102

HOTSPOT

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

A screenshot of a dropdown menu with a downward arrow on the right. The menu is open, showing four options: "Add trusted senders and domains", "Enable domains to protect", "Enable users to protect", and "Phishing email threshold".

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

A screenshot of a dropdown menu with a downward arrow on the right. The menu is open, showing three options: "Add trusted senders and domains", "Enable intelligence for impersonation protection", and "Enable spoof intelligence".

Answer Area:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

QUESTION 103

DRAG DROP

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

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

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

NOTE: Each correct selection is worth one point.

Select and Place:

Policy Types

0 Anti-malware

0 Anti-phishing

0 Anti-spam

0 Safe Attachments

Answer Area

Customize the common attachments filter:

0

Enable impersonation protection for sender domains:

0

Correct Answer:

Policy Types

Answer Area

Customize the common attachments filter:

Enable impersonation protection for sender domains:

Section:

Explanation:

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

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

QUESTION 104

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

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

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

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

Correct Answer: A

Section:

QUESTION 105

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

Block a vulnerable app until the app is updated.

Block an application executable based on a file hash.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

Block a vulnerable app until the app is updated:

An allow or block file
A file indicator
A remediation request
An update ring

Block an application executable based on a file hash:

An allow or block file
A file indicator
A remediation request
An update ring

Answer Area:

Answer Area

Block a vulnerable app until the app is updated:



An allow or block file
A file indicator
A remediation request
An update ring

Block an application executable based on a file hash:

An allow or block file
A file indicator
A remediation request
An update ring

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln-apps>

QUESTION 106

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.

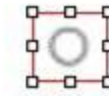
Answer Area:

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 107

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 108

HOTSPOT

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

Contoso.com

East.contoso.com

The forest contains the users shown in the following table.



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

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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



USER SIGN-IN



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

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

Hot Area:

Answer Area

Statements

Yes **No**

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**

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 109

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 110

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 111

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA).

Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

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

Correct Answer: D

Section:

Explanation:

Self-remediation with self-service password reset

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

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



QUESTION 112

You have a Microsoft 365 E5 subscription that contains the following user:

Name: User1
UPN: user1@contoso.com
Email address: user1@marketing.contoso.com
MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in. You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com. What should you do?

- A. Assign an MFA registration policy to User1.
- B. Reset the password of User1.
- C. Add an alternate email address for User1.
- D. Modify the UPN of User1.

Correct Answer: D

Section:

Explanation:

Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>



QUESTION 113

HOTSPOT

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

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

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

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

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

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

Domain and OU filtering

Directory: Refresh Ou/Domain ?

Sync all domains and OUs
 Sync selected domains and OUs

- fabrikam.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Service Accounts
 - OU1
 - OU2
 - Program Data
 - System
 - Users

Previous Next

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

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering


Optional Features

Configure


Filter users and devices


For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

Synchronize all users and devices

Synchronize selected 

FOREST: fabrikam.com

GROUP: 



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

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

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

QUESTION 114

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

Assignments: All users

Controls: Require Azure AD multifactor authentication registration

Enforce Policy: On

On August 3, you create two users named User1 and User2.

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

User	Date
User1	August 5
User2	August 7

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

Hot Area:

User1:

- August 6
- August 17
- August 19
- September 3
- September 5

User2:

- August 8
- August 17
- August 19
- August 21
- September 7



Answer Area:

User1:

▼
August 6
August 17
August 19
September 3
September 5

User2:

▼
August 8
August 17
August 19
August 21
September 7

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>



QUESTION 115

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

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

On-premises Active Directory password complexity policies must be enforced.

Users must be able to use self-service password reset (SSPR) in Azure AD.

What should you use?

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

Correct Answer: D

Section:

Explanation:

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

This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

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

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

Password hash synchronization

Pass-through authentication

Active Directory Federation Services

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

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

QUESTION 116

You have a Microsoft 365 E5 subscription.

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

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

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

What should you configure?

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

Correct Answer: B

Section:

Explanation:

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

Sign-in risk policy

User risk policy

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

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

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

QUESTION 117

HOTSPOT

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

Azure AD Password Protection is configured as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

User1 attempts to update their password to the following passwords:

F@lcon

Project22

T4il\$pin45dg4

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

[Answer choice] will be accepted as a password.

▼

- Only T4il\$pin45dg4
- Only F@lcon and T4il\$pin45dg4
- Only Project22 and T4il\$pin45dg4
- F@lcon, Project22, and T4il\$pin45dg4

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

▼

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

Answer Area:

Answer Area

[Answer choice] will be accepted as a password.

▼

- Only T4il\$pin45dg4
- Only F@lcon and T4il\$pin45dg4
- Only Project22 and T4il\$pin45dg4
- F@lcon, Project22, and T4il\$pin45dg4

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

▼

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

QUESTION 118

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

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

Azure AD Connect has the following settings:

Password Hash Sync: Enabled

Pass-through authentication: Enabled

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

Which users should you identify?

- A. none
- B. Used only1
- C. User1 and User2 only
- D. User1. User2, and User3

Correct Answer: D

Section:

Explanation:

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

QUESTION 119

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

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

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

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

What should you include in the recommendation?

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 120

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

You create an Azure AD tenant.

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

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

What should you include in the recommendation?

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

Correct Answer: A

Section:

Explanation:

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

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



QUESTION 121

You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.

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

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

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

Correct Answer: D

Section:

Explanation:

Retention wins over deletion.

Note:

Explanation for the four different principles:

1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
2. Etc.

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



QUESTION 122

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

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

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

- A. Group1 only
- B. Group1 and Group2 only

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

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 123

HOTSPOT

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

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

Site1 contains the files shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

File1.docx:

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

File2.docx:

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

Answer Area:



Answer Area

File1.docx:

▼
Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

▼
Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

Section:

Explanation:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips>

QUESTION 124

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

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

You need to prevent the users from bypassing the DLP policy.

What should you configure?

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

Correct Answer: D

Section:

Explanation:

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

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



If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

QUESTION 125

HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create retention label

Review and finish

Name
Name
6Months
[Edit](#)

Retention settings
Retention period
6 months
[Edit](#)

Retention action
Retain and Delete
[Edit](#)

Based on
Based on when it was created
[Edit](#)

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

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

- Name
- Info to label
- Create content query
- Scope
- Label
- Finish

Apply label to content matching this query

Conditions

ProjectX

+ Add condition

Back

Next

Cancel

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input checked="" type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

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

QUESTION 126

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

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

Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

This is not a permissions issue.

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

QUESTION 127

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

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

You have a Microsoft 365 E5 subscription.

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

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

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

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>

QUESTION 128

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

A. Yes

B. No

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>



QUESTION 129

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

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

A. only the settings of Policy1

B. only the settings of Policy2

C. only the settings of Policy3

D. no settings

Correct Answer: C

Section:

QUESTION 130

You have a Microsoft 365 E5 tenant.

You configure sensitivity labels.

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

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

What should you do?

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

Correct Answer: B

Section:

QUESTION 131

HOTSPOT

Your company has a hybrid deployment of Microsoft 365.

An on-premises user named User1 is synced to Azure AD.

Azure AD Connect is configured as shown in the following exhibit



Microsoft Azure Active Directory Connect

Welcome

Tasks

Review your solution

Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	ADATUM.COM\MSOL_e785c048abcc

Synchronization Settings

SOURCE ANCHOR mS-DS-ConsistencyGuid	USER PRINCIPAL NAME userPrincipalName
SYNC CRITERIA AlwaysProvision	FILTER OBJECTS TO SYNCHRONIZE BY GROUP Disabled
AZURE AD APP AND ATTRIBUTE FILTERING Disabled	DEVICE WRITEBACK Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC Disabled	EXCHANGE HYBRID DEPLOYMENT Disabled
GROUP WRITEBACK Disabled	PASSWORD HASH SYNCHRONIZATION Enabled
PASSWORD WRITEBACK Disabled	USER WRITEBACK Disabled
AUTO UPGRADE Enabled	EXCHANGE MAIL PUBLIC FOLDERS Disabled
SQL SERVER NAME (localdb)	SQL SERVER INSTANCE NAME .\\ADSync

Previous Exit

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

User1 [answer choice].

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

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

- the password hash will be synchronized to Azure AD
- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

Answer Area:

Answer Area

User1 [answer choice].

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

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

- the password hash will be synchronized to Azure AD
- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

Section:

Explanation:

QUESTION 132

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

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

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From Azure AD Connect, you modify the filtering settings.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 133

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

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

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

What should you configure?

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

Correct Answer: C

Section:

QUESTION 134

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

Several months ago, the Azure AD Connect Health agent was installed on all the servers.

You review the health status of all the servers regularly.

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

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: D, E

Section:

QUESTION 135

HOTSPOT

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

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

You have the named locations shown in the following table.

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

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

* Users or workload identities:

o Include: Group1

o Exclude: Group2

* Cloud apps or actions: Include all cloud apps

* Conditions:

o Include: Any location

o Exclude: Montreal

* Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

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

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

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

Answer Area:

Answer Area

Statements

User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.

Yes **No**

User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.

User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.

Section:

Explanation:

QUESTION 136

HOTSPOT

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

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



You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Hot Area:

Answer Area

Users that can use SSPR:

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

Users that must answer security questions to reset their password:

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

Answer Area:
Answer Area

Users that can use SSPR:

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

Users that must answer security questions to reset their password:

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

Section:
Explanation:

QUESTION 137

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

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

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

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

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

Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 138

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

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

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

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

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

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 139

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

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

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

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

Correct Answer: A, C

Section:

QUESTION 140

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



You create a retention label named Retention1 that is published to all locations.
You need to ensure that User1 can label email messages by using Retention1 as soon as possible.
Which cmdlet should you run in Microsoft Exchange Online PowerShell?

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

Correct Answer: C

Section:

QUESTION 141

HOTSPOT

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

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

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

Sender is condition:

File extension is condition:

Answer Area:

Answer Area

Sender is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

File extension is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

Section:

Explanation:

QUESTION 142

HOTSPOT

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

You need to prevent all users from disabling the policy or reducing the retention period.

How should you configure the Azure PowerShell command? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

- Set-RetentionCompliancePolicy
- Set-ComplianceTag
- Set-HoldCompliancePolicy
- Set-RetentionCompliancePolicy
- Set-RetentionPolicy
- Set-RetentionPolicyTag

-Identity "Policy1"

\$true

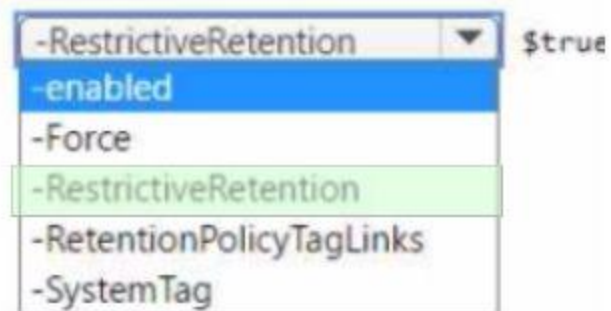
- enabled
- Force
- RestrictiveRetention
- RetentionPolicyTagLinks
- SystemTag

Answer Area:

Answer Area



-Identity "Policy1"



Section:

Explanation:

QUESTION 143

HOTSPOT

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

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

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

- * Retains content for five years
- * Automatically deletes all content that is older than five years

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

- * Applies to content that contains the word Merger
- * Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

```
Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention $true -Force
```

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 144

You have a Microsoft 365 E5 subscription.

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

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

↓ Export

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

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

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

Correct Answer: A

Section:

QUESTION 145

HOTSPOT

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

The subscription has the following two anti-spam policies:

* Name: AntiSpam1

* Priority: 0

* Induce these users, groups and domains

o Users: User3

o Groups: Group1

* Exclude these users, groups and domains

o Groups: Group2

* Message limits

o Set a daily message limit 100

* Name: AntiSpam2

* Priority: 1

* Include these users, groups and domains

o Users: User1 o Groups: Group2

* Exclude these users, groups and domains

o Users: User3

* Message limits

o Set a daily message limit 50

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 can send a maximum of 150 email messages per day.

User2 can send a maximum of 50 email messages per day.

User3 can send a maximum of 100 email messages per day.

Yes

No

Answer Area:

Answer Area

Statements

User1 can send a maximum of 150 email messages per day.

Yes

No

User2 can send a maximum of 50 email messages per day.

User3 can send a maximum of 100 email messages per day.

Section:

Explanation:

QUESTION 146

DRAG DROP

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

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Onboarding method

A local script

Group Policy

Integration with Microsoft Defender for Cloud

Microsoft Intune

Virtual Desktop Infrastructure (VDI) scripts

Device Type

Corporate:

BYOD:

Correct Answer:

Onboarding method

A local script

Group Policy

Virtual Desktop Infrastructure (VDI) scripts

Device Type

Corporate: Microsoft Intune

BYOD: Integration with Microsoft Defender for Cloud

Section:

Explanation:

QUESTION 147

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

- * Admin1
- * Admin2
- * User1

Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

Statements

You can add Admin1 as a member of AU1.

Yes

No

You can add User1 as a member of AU2.

You can assign Admin2 the User administrator role for AU1.

Section:

Explanation:

QUESTION 148

HOTSPOT

You have a Microsoft 365 subscription.

You need to create two groups named Group1 and Group2. The solution must meet the following requirements:

* Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.

* Group2 must support dynamic membership and role assignments but must NOT be mail-enabled.

Which types of groups should you create? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Group1: ▼
Distribution
Dynamic distribution
Microsoft 365
Security

Group2: ▼
Distribution
Dynamic distribution
Microsoft 365
Security

Answer Area:

Answer Area

Group1: ▼
Distribution
Dynamic distribution
Microsoft 365
Security

Group2: ▼
Distribution
Dynamic distribution
Microsoft 365
Security

Section:

Explanation:

QUESTION 149

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.



AU1

Members Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned admins manage group settings.

Add users Add groups Upload users ... Filter

<input type="checkbox"/>	Members	Email address	Last sign-in	Member type
<input type="checkbox"/>	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
<input type="checkbox"/>	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General Assigned Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

[Learn more about assigning admin roles](#)

Add users Add groups

<input type="checkbox"/>	Admin name	Last sign-in	Scope
<input type="checkbox"/>	Group1	Unavailable for groups	Organization
<input type="checkbox"/>	Group2	Unavailable for groups	AU1

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 reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 150

HOTSPOT

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

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

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

* Reset the password of User4.

* Modify the value for the manager attribute of User4.

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

NOTE: Each correct selection is worth one point.

Hot Area:
Answer Area

Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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

Answer Area:
Answer Area



Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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

Section:
Explanation:

QUESTION 151
DRAG DROP

Your company has an Azure AD tenant named contoso.onmicrosoft.com.
You purchase a domain named contoso.com from a registrar and add all the required DNS records.

You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com.

You need to configure User1 to sign in as user1@contoso.com.

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

Select and Place:

Actions

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



Answer Area



Correct Answer:

Actions

- Run Update-MgDomain -DomainId contoso.com.
- Modify the email address of User1.
- Add contoso.com as a SAN for an X.509 certificate.
-
-
-



Answer Area

- Add a custom domain name.
- Verify the custom domain.
- Modify the username of User1.



Section:

Explanation:

Add a custom domain name.

Verify the custom domain.

Modify the username of User1.

QUESTION 152

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

You need to access service health alerts from a mobile phone.

What should you use?

- A. the Microsoft Authenticator app

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

Correct Answer: B

Section:

QUESTION 153

HOTSPOT

You work at a company named Contoso, Ltd.

Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.

Contoso purchases a company named Fabrikam, Inc.

Contoso plans to add the following domains to the Microsoft 365 subscription:

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

You need to ensure that the devices in the new domains can register by using Autodiscover.

How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Vdumps Domains: 3
1
2
3

Enterpriseregistration DNS records: 3
1
2
3

Answer Area:

Answer Area

Domains:

3	▼
1	
2	
3	

Enterpriseregistration DNS records:

3	▼
1	
2	
3	

Section:

Explanation:

QUESTION 154




HOTSPOT

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

Domains

Vdumps

+ Add domain Buy domain Refresh

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

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

NOTE; Each correct selection is worth one point.

Hot Area:

Answer Area

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

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only**
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only**
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Answer Area:

Answer Area

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

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only**
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

- contoso221018.onmicrosoft.com domain only
- contoso221018.onmicrosoft.com domain only**
- contoso221018.onmicrosoft.com domain and all its subdomains only
- contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
- contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Section:

Explanation:

QUESTION 155

You have a Microsoft 365 E5 subscription.

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

* Support KQL for querying data.

* Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. End point analytics
- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

Correct Answer: D

Section:

QUESTION 156

HOTSPOT

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

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

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

* View BitLocker recovery keys.

* Configure the usage location for the users in contoso.com.

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

NOTE: Each correct selection is worth one point



Answer Area

Devices

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

Global

- Global Administrator ⓘ

Identity

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

 Vdumps

Answer:



Answer Area

Devices

Cloud Device Administrator [i](#)

Desktop Analytics Administrator [i](#)

Intune Administrator [i](#)

Printer Administrator [i](#)

Printer Technician [i](#)

Windows 365 Administrator [i](#)

Global

Global Administrator [i](#)

Identity

Application Administrator [i](#)

Application Developer [i](#)

Authentication Administrator [i](#)

Cloud Application Administrator [i](#)

Conditional Access Administrator [i](#)

Domain Name Administrator [i](#)

External Identity Provider Administrator [i](#)

Guest Inviter [i](#)

Helpdesk Administrator [i](#)

Hybrid Identity Administrator [i](#)

License Administrator [i](#)



Hot Area:



Answer Area

Devices

Cloud Device Administrator [i](#)

Desktop Analytics Administrator [i](#)

Intune Administrator [i](#)

Printer Administrator [i](#)

Printer Technician [i](#)

Windows 365 Administrator [i](#)

Global

Global Administrator [i](#)

Identity

Application Administrator [i](#)

Application Developer [i](#)

Authentication Administrator [i](#)

Cloud Application Administrator [i](#)

Conditional Access Administrator [i](#)

Domain Name Administrator [i](#)

External Identity Provider Administrator [i](#)

Guest Inviter [i](#)

Helpdesk Administrator [i](#)

Hybrid Identity Administrator [i](#)

License Administrator [i](#)



Answer Area:



Answer Area

Devices

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

Global

- Global Administrator ⓘ

Identity

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

 Vdumps

Section:

Explanation:

QUESTION 157

DRAG DROP

You have a Microsoft 365 subscription.

You need to review reports to identify the following:

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

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

Select and Place:

Report

- The device usage report in Teams
- The OneDrive usage report
- The SharePoint site usage report
- The Teams usage report in Teams
- The User activity report in Teams

Correct Answer:

Report

- The device usage report in Teams
- The OneDrive usage report
-
-
- The User activity report in Teams

Section:

Explanation:

QUESTION 158

HOTSPOT

You have a Microsoft 365 E5 subscription.

Requirements

- The storage usage of files stored in Microsoft Teams:
- Number of active users per Microsoft Team:



Requirements

- The storage usage of files stored in Microsoft Teams: The SharePoint site usage report
- Number of active users per Microsoft Team: The Teams usage report in Teams

You need to configure a group naming policy.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Portal:
Group types:
Group types:

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

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

Answer Area:

Answer Area

Portal:
Group types:
Group types:

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

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

Section:

Explanation:

QUESTION 159

HOTSPOT

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

Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group1: ▼

- None of the groups
- Group2 only
- Group2 and Group4 only
- Group2, Group4, Group5, and Group6 only
- Group2, Group3, Group4, Group5, and Group6

Group4: ▼

- Group5 only
- None of the groups
- Group5 only
- Group3 and Group5 only
- Group1, Group2, Group3, and Group5 only
- Group1, Group2, Group3, Group5, and Group6

Answer Area:

Answer Area

Group1: ▼

- None of the groups
- Group2 only
- Group2 and Group4 only
- Group2, Group4, Group5, and Group6 only
- Group2, Group3, Group4, Group5, and Group6

Group4: ▼

- Group5 only
- None of the groups
- Group5 only
- Group3 and Group5 only
- Group1, Group2, Group3, and Group5 only
- Group1, Group2, Group3, Group5, and Group6

Section:

Explanation:

QUESTION 160

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to use a mailbox named Mailbox1 to analyze malicious email messages.

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

* Ensure that incoming email is NOT filtered for Mailbox1.

* Detect impersonation and spoofing attacks on all other mailboxes in the subscription.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

Hot Area:









Answer Area

Policies

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






Rules

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







Answer Area:

Answer Area

Policies

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

Rules

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

Section:

Explanation:

QUESTION 161

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

You plan to use Mailbox1 to collect and analyze unfiltered email messages.

You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.

What should you do?

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

Correct Answer: D

Section:

QUESTION 162

HOTSPOT

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

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

* View sync errors in Azure AD Connect Health.

* Configure Azure AD Connect Health settings.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

View sync errors in Azure AD Connect Health:

Configure Azure AD Connect Health settings:

Answer Area:

Answer Area

View sync errors in Azure AD Connect Health:

Configure Azure AD Connect Health settings:

Section:

Explanation:

QUESTION 163

HOTSPOT

Your network contains an Active Directory domain and an Azure AD tenant.
You implement directory synchronization for all 10,000 users in the organization.
You automate the creation of 100 new user accounts.
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.
Which command should you run? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

<input type="text" value="Start-ADSyncSyncCycle"/>	-PolicyType	<input type="text" value="Delta"/>
<input type="text" value="Start-ADSyncSyncCycle"/>		<input type="text" value="Delta"/>
<input type="text" value="Set-ADSyncScheduler"/>		<input type="text" value="Initial"/>
<input type="text" value="Invoke-ADSyncRunProfile"/>		<input type="text" value="Full"/>

Answer Area:

Answer Area

<input type="text" value="Start-ADSyncSyncCycle"/>	-PolicyType	<input type="text" value="Delta"/>
<input type="text" value="Start-ADSyncSyncCycle"/>		<input type="text" value="Delta"/>
<input type="text" value="Set-ADSyncScheduler"/>		<input type="text" value="Initial"/>
<input type="text" value="Invoke-ADSyncRunProfile"/>		<input type="text" value="Full"/>

Section:

Explanation:

QUESTION 164

HOTSPOT

You have a Microsoft 365 Enterprise E5 subscription.
You add a cloud-based app named App1 to the Azure AD enterprise applications list.
You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.
Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

New ...

Conditional Access policy

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

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

Name *

App1 policy ✓

What does this policy apply to?

Users and groups ✓

Assignments

Users or workload identities ⓘ
All users

Include Exclude

- None
- All users
- Select users and groups

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected ✓

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

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected ✓

Session ⓘ

0 controls selected

Enable policy

Report-only On Off ✓

Answer Area:

Answer Area

New ...

Conditional Access policy

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

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

Name *

 ✓

What does this policy apply to?

 ✓

Assignments

Users or workload identities ⓘ

All users

Include Exclude

None

All users

Select users and groups

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected ✓

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

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected ✓

Session ⓘ

0 controls selected

Enable policy

Report-only On Off ✓

Section:
Explanation:

QUESTION 165

HOTSPOT

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

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

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

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

Microsoft Authenticator settings ... ×

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

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

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 166

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

* Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources

* Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Password Hash Synchronization
- B. Password writeback
- C. Directory extension attribute sync
- D. Enable single sign-on
- E. Pass-through authentication

Correct Answer: A, B

Section:

QUESTION 167

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

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

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

What should you include in the recommendation?

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

Correct Answer: D

Section:

QUESTION 168

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Sign-in risk policy:

Leaked credentials
Atypical travel
Leaked credentials
Possible attempt to access Primary Refresh Token (PRT)

User risk policy:

Malicious IP address
Leaked credentials
Malicious IP address
Suspicious browser

Answer Area:

Answer Area

Sign-in risk policy:

- Atypical travel
- Leaked credentials**
- Possible attempt to access Primary Refresh Token (PRT)

User risk policy:

- Leaked credentials
- Malicious IP address**
- Suspicious browser

Section:

Explanation:

QUESTION 169

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.

You need to reduce false positives for impossible travel when the users sign in from the corporate network.

What should you configure?

- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations
- D. user risk policies

Correct Answer: C

Section:

QUESTION 170

HOTSPOT

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

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

User1: ▼
Email address only
Phone number only
Security questions only
Phone number and email address

User2: ▼
Email address only
Phone number only
Security questions only
Phone number and email address

User3: ▼
Email address only
Phone number only
Security questions only
Phone number and email address



Answer Area:
Answer Area

User1: ▼
Email address only
Phone number only
Security questions only
Phone number and email address

User2: ▼
Email address only
Phone number only
Security questions only
Phone number and email address

User3: ▼
Email address only
Phone number only
Security questions only
Phone number and email address

Section:

Explanation:

QUESTION 171

You have a Microsoft 365 E5 subscription.

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

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

Which authentication method should you use?

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

Correct Answer: C

Section:

QUESTION 172

HOTSPOT

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.

Username ⓘ	Last activation date (UTC)	Last activity date (UTC)	Choose columns
431B8D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022	
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

You need ensure that the report meets the following requirements:

* The Username column must display the actual name of each user.

* Usage of the Microsoft Teams mobile app must be displayed.

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

Hot Area:

Answer Area

The Username column must display the actual name of each user:

Reports in Org settings
Privacy profile in Org settings
Reports in Org settings
The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings
Microsoft Teams in Org settings
The columns in the report
The Teams license assignment

Answer Area:

Answer Area

The Username column must display the actual name of each user:

Reports in Org settings
Privacy profile in Org settings
Reports in Org settings
The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings
Microsoft Teams in Org settings
The columns in the report
The Teams license assignment

Section:

Explanation:

QUESTION 173

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

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

- A. User2 and User4 only
- B. User1 and User3 only

- C. User1 only
- D. User1, User2, User3, and User4

Correct Answer: C

Section:

QUESTION 174

HOTSPOT

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

Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.

The subscription has the following Conditional Access policy:

* Name: Policy1

* Assignments

o Users and groups: Group1, Group2

o Cloud apps or actions: All cloud apps

* Access controls

o Grant Require multi-factor authentication

* Enable policy: On

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



Microsoft Authenticator settings



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

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

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups



Add groups

Name	Type	Registration	Authentication mode	
Group1	Group	Optional	Passwordless	X
Group2	Group	Optional	Passwordless	X

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 sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 175

HOTSPOT

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

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

The Azure AD password policy is configured as shown in the following exhibit.

Password policy

Set the password policy for all users in your organization.

Days before passwords expire 90

Days before a user is notified about 14
expiration

You confirm that User1 is synced to Azure AD.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

dumps

Answer Area

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

Section:

Explanation:

QUESTION 176

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

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

* Signs in to Microsoft Exchange Online from an anonymous IP address

* Signs in to Microsoft SharePoint Online from a device in New York City.

* Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

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

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

Correct Answer: A

Section:

QUESTION 177

HOTSPOT

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

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

The subscription contains the role assignments shown in the following table.



Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

Hot Area:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 178

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named user1@contoso.com and user2@contoso.com and a Microsoft SharePoint site named Site1.

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

Name	Content contains	User notifications	Priority
Rule1	4 or more IP addresses	User1@contoso.com	0
Rule2	2 or more IP addresses	User1@contoso.com	1
Rule3	3 or more IP addresses	User2@contoso.com	2

DLP1 is applied to Site1.

You have the files shown in the following table.

Name	Number of IP addresses in the file
File1.xlsx	2
File2.doc	3
File3.pptx	4
File4.txt	6

You copy the files to Site1.

How many notifications will each user receive? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1@contoso.com:

0
1
2
3
4
5
6
7
8

User2@contoso.com:

0
1
2
3
4
5
6
7
8

Vdumps

Answer Area:

Answer Area

User1@contoso.com:

0
1
2
3
4
5
6
7
8

User2@contoso.com:

0
1
2
3
4
5
6
7
8

Section:

Explanation:

QUESTION 179

HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name	Managers
	Description	
	Applied to	If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com
		Edit
	Safety tips > User impersonation	Off
	Safety tips > Domain impersonation	Off
	Safety tips > Unusual characters	Off
	Mailbox intelligence	Off
		Edit
Spooof	Enable antispoofing protection	On
	Action	Quarantine the message
		Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive
		Edit



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

If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages is moved to the Junk Email folder
- the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

Answer Area:

Answer Area

If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages is moved to the Junk Email folder
- the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Domain impersonation
- Enable antispooofing protection
- Mailbox intelligence

Section:

Explanation:

QUESTION 180

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure threat protection for Microsoft 365 to meet the following requirements:

- * Limit a user named User 1 from sending more than 30 email messages per day.
- * Prevent the delivery of a specific file based on the file hash.

Which two threat policies should you configure in Microsoft Defender for Office 365? To answer, select the appropriate threat policies in the answer area.






NOTE: Each correct selection is worth one point.

Hot Area:









Answer Area

Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps



Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own







Answer Area:

Answer Area

Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected.
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps.

Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users.
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first.
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own.

Section:

Explanation:

QUESTION 181

HOTSPOT

Your company has a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
User1	Privileged Role Administrator
User2	User Administrator
User3	Security Administrator
User4	Billing Administrator

The tenant includes a security group named Admin1. Admin1 will be used to manage administrative accounts. External collaboration settings have default configuration. You need to identify which users can perform the following administrative tasks:

Hot Area:

Answer Area

Create guest user accounts:

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

Add User3 to Admin1:

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

Answer Area:

Answer Area

Create guest user accounts:

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

Add User3 to Admin1:

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

Section:

Explanation:

QUESTION 182

HOTSPOT

You have a Microsoft 365 subscription that uses a domain name of adatum.com.

In Microsoft Entra ID, you set Guest invite restrictions to Only users assigned to specific admin roles can invite guest users.

A user named used@adatum.com reports that they can no longer invite external users from a domain named contoso.com to collaborate in Microsoft Teams.

You need to modify the Microsoft Entra ID configuration to meet the following requirements:

- * Ensure that User1 can invite the contoso.com users to Teams
- * Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant.
- * Follow the principle of least privilege

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

Hot Area:

Answer Area

Ensure that User1 can invite the contoso.com users to Teams:

- Assign the Guest Inviter role to User1.
- Assign the User Administrator role to User1.
- Assign the Teams Administrator role to User1.
- Add User1 as a group owner to each team in Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant:

- From the Cross-tenant access settings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings.
- From the External collaboration settings, edit the Guest user access restrictions settings.

Answer Area:

Answer Area

Ensure that User1 can invite the contoso.com users to Teams:

- Assign the Guest Inviter role to User1.
- Assign the User Administrator role to User1.
- Assign the Teams Administrator role to User1.
- Add User1 as a group owner to each team in Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant:

- From the Cross-tenant access settings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings.
- From the External collaboration settings, edit the Guest user access restrictions settings.

Section:

Explanation: