

MS-101.77q

Number: MS-101
Passing Score: 800
Time Limit: 120 min

MS-101

Microsoft 365 Mobility and Security

Implement modern device services

Question Set 1

QUESTION 1

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

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

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

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

You configure pilot co-management.

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

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

Solution: You add Device1 to an Active Directory group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://www.sccconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/>

QUESTION 2

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

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

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

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

You configure pilot co-management.

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

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

Solution: You unjoin Device1 from the Active Directory domain.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. computers that have biometric hardware features
- B. Microsoft Intune enrollment
- C. Microsoft Azure Active Directory (Azure AD)
- D. smartcards
- E. TPM-enabled devices

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-ssso-base>

QUESTION 4

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.

What should you configure?

- A. Enrollment restrictions from the Intune admin center
- B. device enrollment managers from the Intune admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 5

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/sccm/comanage/overview>

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles>

QUESTION 6

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You have a Microsoft 365 subscription.

You need to ensure that users can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

- A. the Enrollment restrictions
- B. the mobile device management (MDM) authority
- C. the Exchange on-premises access settings
- D. the Windows enrollment settings

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/intune/mdm-authority-set>

QUESTION 7

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the **Locations** tab.)

The users and groups settings are configured as shown in the Users and Groups exhibit. (Click **Users and Groups** tab.)

Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

- A. From the conditional access policy, configure the device state.
- B. From the Azure Active Directory admin center, create a custom control.
- C. From the Device Management admin center, create a device compliance policy.

D. From the Azure Active Directory admin center, create a named location.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 8

You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

References:

<https://insider.windows.com/en-us/for-business-organization-admin/>

QUESTION 9

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Cloud application administrator
- B. Application administrator
- C. Global administrator
- D. Service administrator

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 10

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

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

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

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

You configure pilot co-management.

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

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

Solution: You add Device1 to a Configuration Manager device collection.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

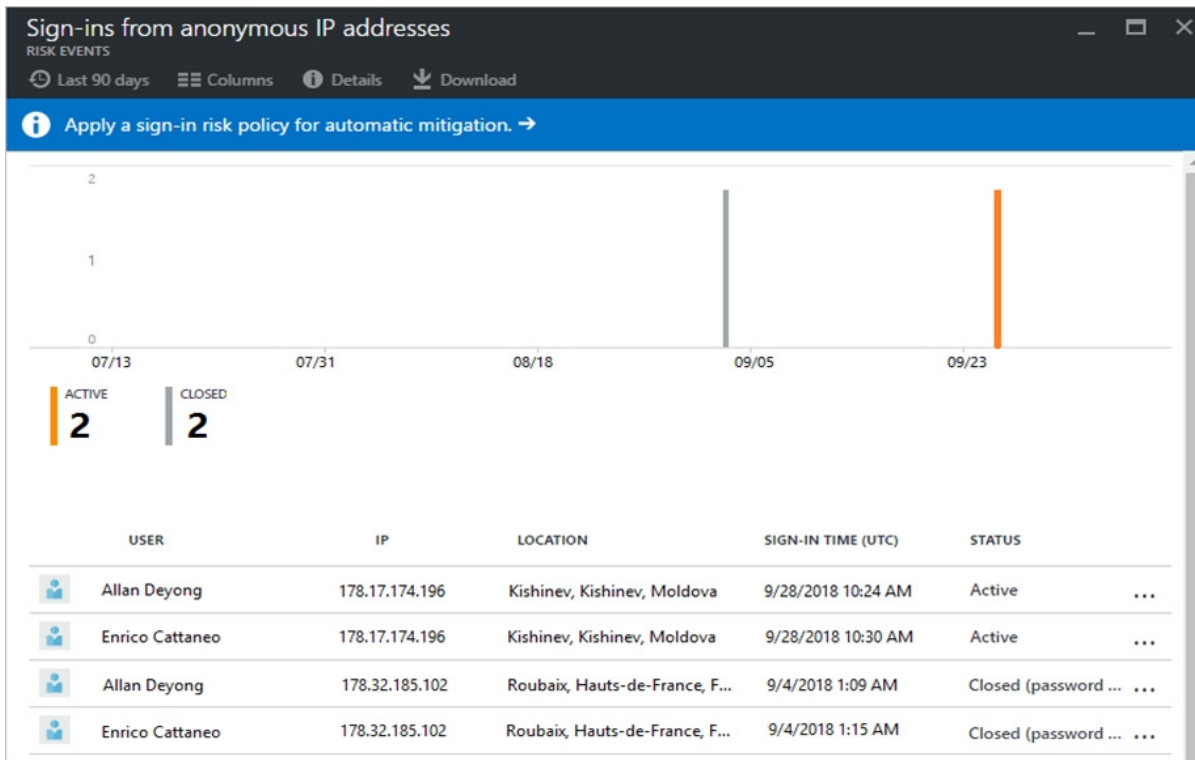
Explanation

Explanation/Reference:

QUESTION 12

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk

events shown in the exhibit. (Click the **Exhibit** tab.)



You need to reduce the likelihood that the sign-ins are identified at risky.

What should you do?

- A. From the Security & Compliance admin center, create a classification label.
- B. From the Security & Compliance admin center, add the users to the Security Readers role group.
- C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 13

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 from the Security & Compliance admin center?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the default safe links policy.
- 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: (none)
Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients>

QUESTION 14

You have a Microsoft 365 tenant.

You have a line-of-business application named App1 that users access by using the My Apps portal.

After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.

You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.

What should you do?

- A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
- B. From Microsoft Cloud App Security, modify the impossible travel alert policy.
- C. From Microsoft Cloud App Security, create an app discovery policy.
- D. From the Azure Active Directory admin center, modify the conditional access policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

References:

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

QUESTION 15

A user receives the following message when attempting to sign in to <https://myapps.microsoft.com>:

“Your sign-in was blocked. We’ve detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.”

Which configuration prevents the users from signing in?

- A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies
- B. Microsoft Azure Active Directory (Azure AD) conditional access policies
- C. Security & Compliance supervision policies
- D. Security & Compliance data loss prevention (DLP) policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

References:

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

QUESTION 16

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

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

- The Assignments settings are configured as follows:
 1. Users and groups: Group1
 2. Cloud apps: Microsoft Office 365 Exchange Online
 3. Conditions: Include All device state, exclude Device marked as compliant
- Access controls is set to Block access.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.

You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.

You need to recommend a Windows 10 deployment method.

What should you recommend?

- A. a provisioning package
- B. an in-place upgrade
- C. wipe and load refresh
- D. Windows Autopilot

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

QUESTION 18

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.

Your company uses the following types of devices:

- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

- A. Windows 10 and Windows 8.1 only
- B. Windows 10, Android, and iOS only
- C. Windows 10 only
- D. Windows 10, Windows 8.1, Android, and iOS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

QUESTION 19

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

- A. Windows Autopilot

- B. Windows Update
- C. Subscription Activation
- D. an in-place upgrade

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

QUESTION 20

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

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

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

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

You configure pilot co-management.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Implement modern device services

Testlet 2

Case Study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	<i>None</i>
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements

Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

QUESTION 1

You need to create the Microsoft Store for Business.

Which user can create the store?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 2

You need to ensure that User1 can enroll the devices to meet the technical requirements.

What should you do?

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

Implement Microsoft 365 security and threat management

Question Set 1

QUESTION 1

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

- A. Click **Investigate**, and then click **Activity log**.
- B. Click **Control**, and then click **Policies**. Create a file policy.
- C. Click **Discover**, and then click **Create snapshot report**.
- D. Click **Investigate**, and then click **Files**.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas>

QUESTION 2

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 Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United States.

You plan to onboard all the devices to Windows Defender ATP.

You need to store the Windows Defender ATP data in Europe.

What should you first?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Exchange admin center, create an anti-malware policy.

D. From the Exchange admin center, create a spam filter policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection>

QUESTION 4

Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP.

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

- A. From Azure ATP, configure the notifications and reports.
- B. From Azure ATP, configure the data sources.
- C. From Windows Defender Security Center, configure the Machine management settings.
- D. From Windows Defender Security Center, configure the General settings.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 5

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the score.

What should you configure from the Cloud Discover settings?

- A. Organization details
- B. Default behavior
- C. Score metrics
- D. App tags

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries>

QUESTION 6

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the **BEST** answer.

- A. Deploy an Azure ATP sensor, and then configure port mirroring.
- B. Deploy an Azure ATP sensor, and then configure detections.
- C. Deploy an Azure ATP standalone sensor, and then configure detections.
- D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

QUESTION 7





DRAG DROP

You create a Microsoft 365 subscription.

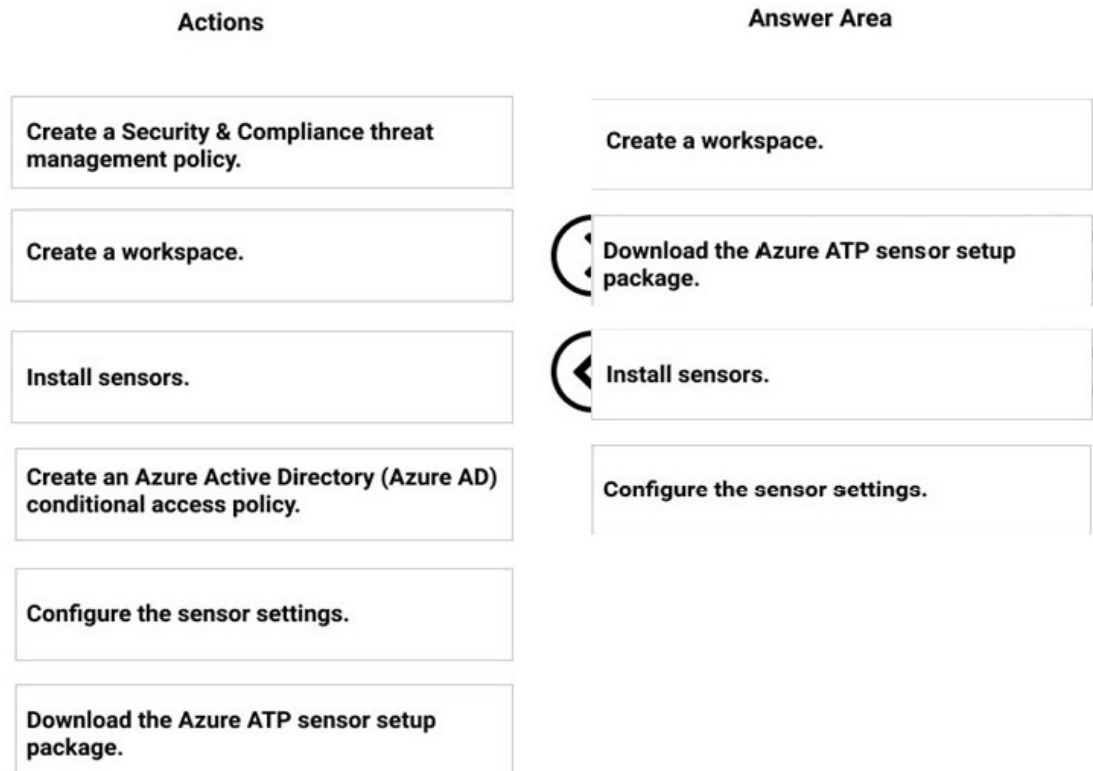
You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

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

Select and Place:

Actions		Answer Area
Create a Security & Compliance threat management policy.		
Create a workspace.		
Install sensors.		
Create an Azure Active Directory (Azure AD) conditional access policy.		
Configure the sensor settings.		
Download the Azure ATP sensor setup package.		

Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

References:

<https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/>

QUESTION 8

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

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

Updates

Domain Controller restart during updates ? OFF						
NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED DEPLOYMENT	STATUS	
LON-DC1	Sensor	2.48.5521	ON	ON	Up to date	

Save

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

- A. 1 hour
- B. 12 hours
- C. 48 hours
- D. 7 days
- E. 24 hours

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 9

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal.

You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.

What should you do?

- A. From the Device Management admin center, configure conditional access settings.
- B. From the Azure Active Directory admin center, configure the device settings.
- C. From the Azure Active Directory admin center, configure the organizational relationships settings.
- D. From the Device Management admin center, configure Exchange on-premises access settings.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Device Management admin center, you create a trusted location and a compliance policy

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678>

QUESTION 12

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A>

QUESTION 13

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

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

You have a Microsoft 365 subscription.

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

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This solution applies to users accessing Azure Active Directory, not to users accessing SharePoint Online. Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

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

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678>

QUESTION 14

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?

- A. From the Security & Compliance admin center, create a label and a label policy.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Exchange admin center, start a mail flow message trace.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

QUESTION 15

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription.

You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents

stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a safe attachments policy.
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- D. From the Security & Compliance admin center, create an alert policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 18

You have a Microsoft Azure Active Directory (Azure AD) tenant.

The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Global administrator
- B. Cloud application administrator
- C. Application administrator
- D. Service administrator

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 19

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

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Implement Microsoft 365 security and threat management

Testlet 2

Case Study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	<i>None</i>
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements

Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

QUESTION 1

On which server should you install the Azure ATP sensor?

- A. Server1
- B. Server2
- C. Server3
- D. Server4
- E. Server5

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

Manage Microsoft 365 governance and compliance

Question Set 1

QUESTION 1

Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

- A. a Security & Compliance data loss prevention (DLP) policy
- B. a Microsoft Cloud App Security access policy
- C. a Security & Compliance retention policy
- D. a Microsoft Cloud App Security file policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 2

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- A. From the Security & Compliance admin center, create an alert policy.
- B. From the SharePoint site, create an alert.
- C. From the SharePoint admin center, modify the sharing settings.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 3

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

- A. Run the `Set-AadrmOnboardingControlPolicy` cmdlet.
- B. Run the `Add-AadrmRoleBasedAdministrator` cmdlet.
- C. Create an Azure Information Protection policy.
- D. Configure the protection activation status for Azure Information Protection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/>

QUESTION 4

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
- Opened a mailbox of which the user was not the owner
- Reset a user password

What should you use?

- A. Microsoft Azure Activity Directory (Azure AD) audit logs
- B. Security & Compliance content search
- C. Microsoft Azure Activity Directory (Azure AD) sign-ins
- D. Security & Compliance audit log search

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

QUESTION 5

You have a Microsoft 365 subscription.

You have a user named User1.

You need to ensure that User1 can place a hold on all mailbox content.

Which role should you assign to User1?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>

QUESTION 6

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E3 license.

You enable auditing for your organization.

What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- A. 2 years
- B. 1 year
- C. 30 days
- D. 90 days

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 7

HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

Review your settings

Template name

U.K. Personally Identifiable Information (PII) Data

Edit

Policy name

U.K. Personally Identifiable Information (PII) Data

Edit

Description

Edit

Applies to content in these locations

Exchange email
 SharePoint sites
 OneDrive accounts

Edit

Policy settings

If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

 If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Edit

Turn policy on after it's created?

Yes

Edit

Back

Create

Cancel

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 user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be **[answer choice]**.

▼

allowed

blocked without warning

blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be **[answer choice]**.

▼

allowed

blocked without warning

blocked, but the user can override the policy

Correct Answer:

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

▼
allowed
blocked without warning
blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

▼
allowed
blocked without warning
blocked, but the user can override the policy

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 8

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 9

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?

- A. From the Security & Compliance admin center, create an eDiscovery case.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Microsoft Cloud App Security, create an access policy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case>

QUESTION 10

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

- A. From the SharePoint admin center, configure hybrid search.
- B. From the SharePoint admin center, create a managed property.
- C. From the Security & Compliance Center PowerShell, run the `New-DataClassification` cmdlet.
- D. From the Security & Compliance Center PowerShell, run the `New-DlpComplianceRule` cmdlet.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps>

QUESTION 11

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the work ProjectX.

You need to export the results of the content search.

What do you need to download the report?

- A. a certification authority (CA) certificate
- B. an export key
- C. a password
- D. a user certificate

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

QUESTION 12

Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

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

What should you create?

- A. a mail flow rule from the Exchange admin center
- B. a message trace from the Security & Compliance admin center
- C. a supervision policy from the Security & Compliance admin center
- D. a sharing policy from the Exchange admin center

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules>

QUESTION 13

You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

- A. Azure ATP
- B. Security & Compliance
- C. Cloud App Security
- D. Flow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 14

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 Online.

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

What should you configure?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 15

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

What should you do?

- A. From the SharePoint Online admin center, view the usage reports.
- B. From the Security & Compliance admin center, perform an audit log search.
- C. From the Microsoft 365 admin center, view the usage reports.
- D. From the Microsoft 365 admin center, view the properties of the user's user account.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 16

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the **Exhibit** tab.)

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

- ☒ Block people from sharing and restrict access to shared content
By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content. Block these people from accessing SharePoint and OneDrive content
- ☐ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access
- ☒ Only people outside your organization. People inside your organization will continue to have access.
- ☐ Encrypt email messages (applies only to content in Exchange)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

- A. an exception
- B. an action
- C. a condition
- D. a group

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 17

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

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

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

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, 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: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search>

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps>

QUESTION 18

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

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

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, 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-AzureRmRoleAssignment` cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new-azuremroleassignment?view=azurermps-6.13.0>

QUESTION 19

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

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

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

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

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator
User5	None	None

Microsoft Store for Business has the following Shopping behavior settings:

- **Allow users to shop** is set to **On**
- **Make everyone a Basic Purchaser** is set to **Off**

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

- A. User1, User2, User3, User4, and User5
- B. User1 only

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

References:

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

QUESTION 21

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Security Administrator
- B. Records Management
- C. Compliance Administrator
- D. eDiscovery Manager

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager>

QUESTION 22

You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Exchange admin center, create a public folder.
- B. Copy the PST files by using AzCopy.
- C. From the Exchange admin center, assign admin roles.
- D. From the Microsoft Azure portal, create a storage account that has a blob container.
- E. From the Microsoft 365 admin center, deploy an add-in.
- F. Create a mapping file that uses the CSV file format.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files>

QUESTION 23

HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ✓ Settings
- ✓ Choose locations
- Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name: contoso [Edit](#)

Description: [Edit](#)

Applies to content in these locations [Edit](#)

- Exchange email
- OneDrive accounts
- SharePoint sites
- Office 365 groups

Settings [Edit](#)

Retention period: Don't retain content, but delete it if it's older than 7 years

⚠ Content that's currently older than 7 years will be deleted after you turn on the policy

[Back](#) [Save for later](#) [Create this policy](#) [Cancel](#)

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

Microsoft SharePoint files that are affected by the policy will be [answer choice].

	▼
recoverable for up to seven years	
deleted seven years after they were created	
retained for only seven years from when they were created	

Once the policy is created, [answer choice].

	▼
some data may be deleted immediately	
data will be retained for a minimum of seven years	
users will be prevented from permanently deleting email messages for seven years	

Correct Answer:

Answer Area

Microsoft SharePoint files that are affected by the policy will be [answer choice].

▼
recoverable for up to seven years
deleted seven years after they were created
retained for only seven years from when they were created

Once the policy is created, [answer choice].

▼
some data may be deleted immediately
data will be retained for a minimum of seven years
users will be prevented from permanently deleting email messages for seven years

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

- A. From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
- B. From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
- C. From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
- D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. However, the super user feature is not enabled by default. The PowerShell cmdlet Enable-AadrmSuperUserFeature is used to manually enable the super user feature.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users>

QUESTION 25

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Cloud App Security admin center, you create an access policy.

Does this meet the goal?

- A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User4 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

References:

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

QUESTION 27

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User3 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

Reference:

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

QUESTION 28

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Exchange admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

- A. A conditional access policy.
- B. A compliance policy.
- C. An app protection policy.
- D. An app configuration policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/intune/app-protection-policy>

QUESTION 30

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User1 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only Azure ATP administrators can modify the sensors.

References:

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

QUESTION 32

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
- B. An administrator creates a new mail flow rule.
- C. A user shares a Microsoft SharePoint folder with an external user.
- D. A user delegates permissions to their mailbox.
- E. A user purges messages from their mailbox.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c>

Manage Microsoft 365 governance and compliance

Testlet 2

Case Study

Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment

Current Infrastructure

ADatum 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.adatum.com.

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

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

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

Requirements

Business Goals

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

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

Technical Requirements

ADatum 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 365 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 U.S. 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

Which report should the New York office auditors view?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 2

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

What should you create?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

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: C

Section: (none)

Explanation

Explanation/Reference:

References:

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