



MS-101.58q

MS-101

MS-101

Microsoft 365 Mobility and Security

Score: 800/1000

Version:

Time Limit: 120 Minutes

Implement modern device services

(20 questions)

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?

- ☐ Yes
- ☐ No

Question 2

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?

- ☐ Microsoft Azure Active Directory (Azure AD) Identity Protection policies
- ☐ Microsoft Azure Active Directory (Azure AD) conditional access policies
- ☐ Security & Compliance supervision policies
- ☐ Security & Compliance data loss prevention (DLP) policies

Question 3

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?

- ☐ Windows Autopilot
- ☐ Windows Update
- ☐ Subscription Activation
- ☐ an in-place upgrade

Question 4

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

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

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 create a device configuration profile from the Intune admin center.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 5

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

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

You 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?

- ☐ Yes
- ☐ No

Question 6

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?

- ☐ Windows 10 and Windows 8.1 only
- ☐ Windows 10, Android, and iOS only
- ☐ Windows 10 only
- ☐ Windows 10, Windows 8.1, Android, and iOS

Question 7

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.

- ☐ Deploy applications to Windows 10 devices.
- ☐ Deploy VPN profiles to iOS devices.
- ☐ Deploy VPN profiles to Windows 10 devices.
- ☐ Publish applications to Android devices.

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.

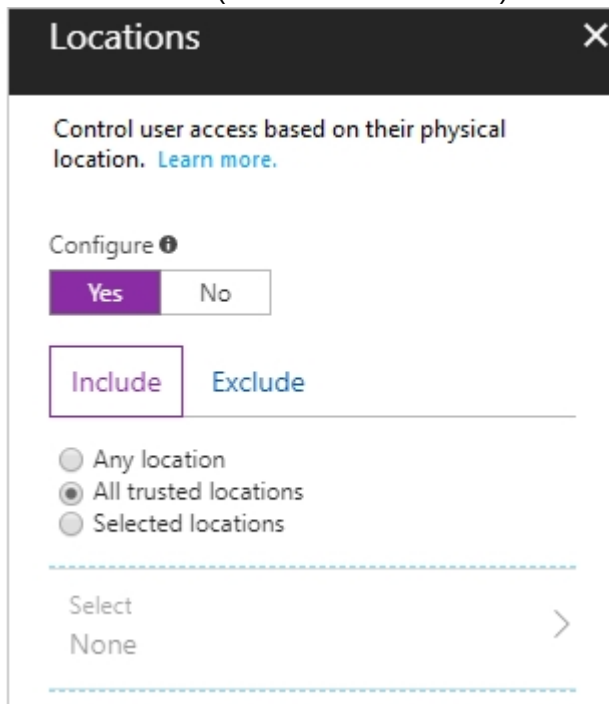
Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

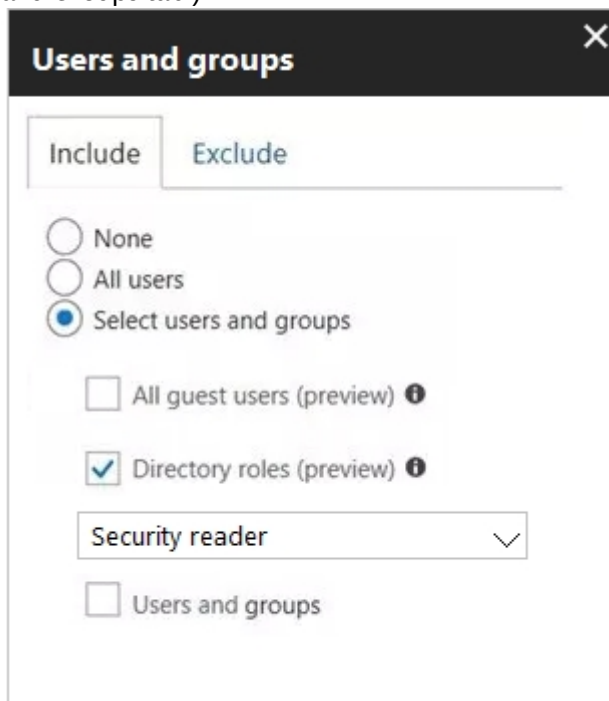
- ☐ Select when Quality Updates are received
- ☐ Select when Preview Builds and Feature Updates are received
- ☐ Turn off auto-restart for updates during active hours
- ☐ Manage preview builds
- ☐ Automatic updates detection frequency

Question 9

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 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?

- ☐ From the conditional access policy, configure the device state.
- ☐ From the Azure Active Directory admin center, create a custom control.
- ☐ From the Intune admin center, create a device compliance policy.
- ☐ From the Azure Active Directory admin center, create a named location.

Question 10

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?

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

Question 11

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.

- ☐ computers that have biometric hardware features
- ☐ Microsoft Intune enrollment
- ☐ Microsoft Azure Active Directory (Azure AD)
- ☐ smartcards
- ☐ TPM-enabled devices

Question 12

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

You have a Microsoft 365 subscription.

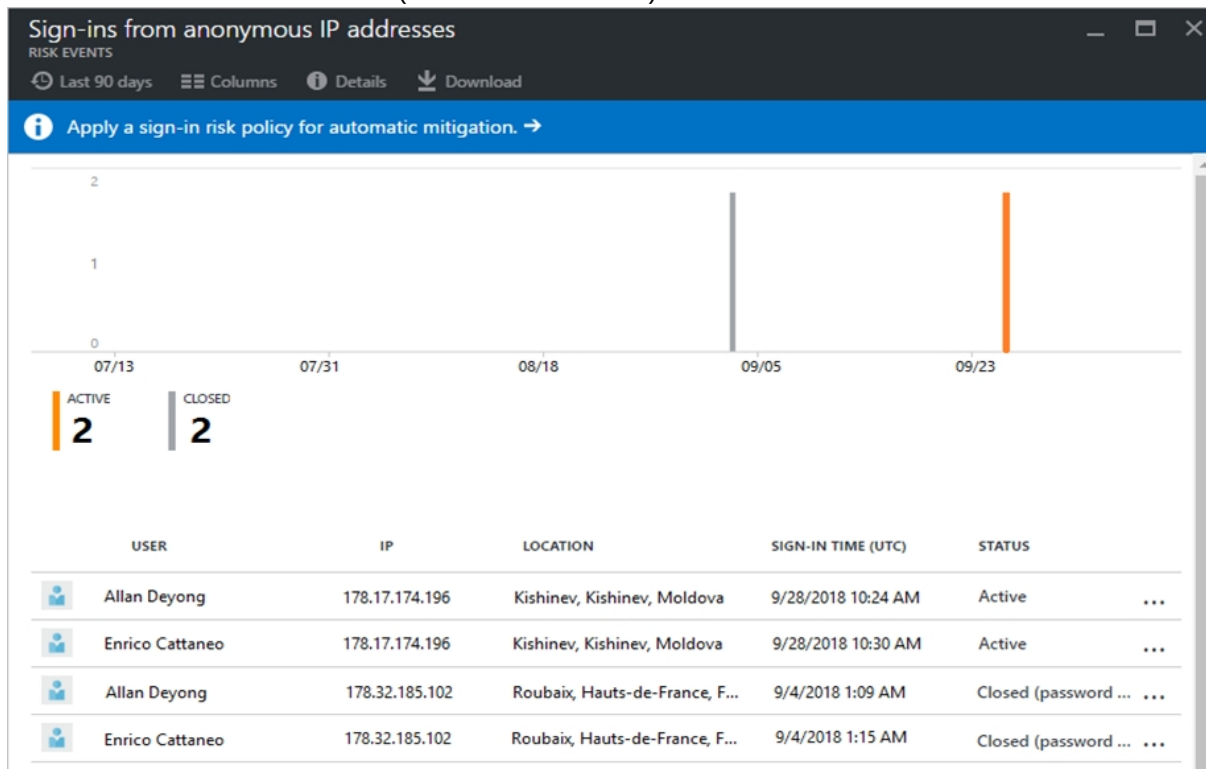
You need to ensure that users can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

- ☐ the Enrollment restrictions
- ☐ the mobile device management (MDM) authority
- ☐ the Exchange on-premises access settings
- ☐ the Windows enrollment settings

Question 13

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 as risky.

What should you do?

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

Question 14

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?

- ☐ Yes
- ☐ No

Question 15

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?

- ☐ Create a data loss prevention (DLP) policy that has a Content is shared condition.
- ☐ Modify the default safe links policy.
- ☐ Create a data loss prevention (DLP) policy that has a Content contains condition.
- ☐ Create a new safe links policy.

Question 16

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 provisioning package
- ☐ an in-place upgrade
- ☐ wipe and load refresh
- ☐ Windows Autopilot

Question 17

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?

- ☐ Enrollment restrictions from the Intune admin center
- ☐ device enrollment managers from the Intune admin center
- ☐ MAM User scope from the Azure Active Directory admin center
- ☐ MDM User scope from the Azure Active Directory admin center

Question 18

HOTSPOT

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Answer Area

First action to perform:

▼ Enroll the devices in Microsoft Intune. Configure device compliance in Microsoft Intune. Create a Microsoft Azure Log Analytics workspace. Add an alias (CNAME) record to the DNS zone of contoso.com.
--

Second action to perform:

▼ Configure all the devices to have a commercial ID. Configure software inventory in Configuration Manager. Configure all the devices to join the Windows Insider Program. Configure and restart the Windows Update service on all the devices.

Question 19

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?

- ☐ Cloud application administrator
- ☐ Application administrator
- ☐ Global administrator
- ☐ Service administrator

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: You unjoin Device1 from the Active Directory domain.

Does this meet the goal?

- ☐ Yes
- ☐ No

Case Study (3 questions)

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 device
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 21

You need to create the Microsoft Store for Business.

Which user can create the store?

- ☐ User2
- ☐ User3
- ☐ User4
- ☐ User5

Question 22

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

What should you do?

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

Question 23

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- ☐ 1
- ☐ 4
- ☐ 7
- ☐ 31

Implement Microsoft 365 security and threat management

(13 questions)

Question 24

DRAG DROP

You create a Microsoft 365 subscription.

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

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

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

Question 25

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?

- ☐ 1 hour
- ☐ 12 hours
- ☐ 48 hours
- ☐ 7 days
- ☐ 24 hours

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 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?

- ☐ Yes
- ☐ No

Question 27

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender Advanced Threat Protection (ATP).

You need to create a filtered view that displays which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

- ☐ the threat intelligence API
- ☐ Automated investigations
- ☐ Threat analytics
- ☐ Advanced hunting

Question 28

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.

- ☐ Deploy an Azure ATP sensor, and then configure port mirroring.
- ☐ Deploy an Azure ATP sensor, and then configure detections.
- ☐ Deploy an Azure ATP standalone sensor, and then configure detections.
- ☐ Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Question 29

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?

- ☐ Yes
- ☐ No

Question 30

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?

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

Question 31

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?

- ☐ Click Investigate, and then click Activity log.
- ☐ Click Control, and then click Policies. Create a file policy.
- ☐ Click Discover, and then click Create snapshot report.
- ☐ Click Investigate, and then click Files.

Question 32

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

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

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?

- ☐ Yes
- ☐ No

Question 33

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

You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to an untrusted device.

What should you do?

- ☐ From the Intune admin center, configure the Conditional access settings.
- ☐ From the Azure Active Directory admin center, configure the Organizational relationships settings.
- ☐ From the Azure Active Directory admin center, configure the Application proxy settings.
- ☐ From the Azure Active Directory admin center, configure the Devices settings.

Question 34

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?

- ☐ Organization details
- ☐ Default behavior
- ☐ Score metrics
- ☐ App tags

Question 35

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?

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

Question 36

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?

- ☐ Create a workspace.
- ☐ Onboard a new device.
- ☐ Delete the workspace.
- ☐ Offboard the test devices.

Case Study (1 questions)

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 shown 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 uses. 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 37

You need to meet the technical requirement for large-volume document retrieval.

What should you create?

- ☐ an activity policy from Microsoft Cloud App Security
- ☐ a data loss prevention (DLP) policy from the Security & Compliance admin center
- ☐ a file policy from Microsoft Cloud App Security
- ☐ an alert policy from the Security & Compliance admin center

Manage Microsoft 365 governance and compliance

(18 questions)

Question 38

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?

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

Question 39

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?

- ☐ Microsoft Azure Activity Directory (Azure AD) audit logs
- ☐ Security & Compliance content search
- ☐ Microsoft Azure Activity Directory (Azure AD) sign-ins
- ☐ Security & Compliance audit log search

Question 40

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?

- ☐ Azure ATP
- ☐ Security & Compliance
- ☐ Cloud App Security
- ☐ Flow

Question 41

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?

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

Question 42

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 Security & Compliance data loss prevention (DLP) policy
- ☐ a Microsoft Cloud App Security access policy
- ☐ a Security & Compliance retention policy
- ☐ a Microsoft Cloud App Security file policy

Question 43

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 certification authority (CA) certificate
- ☐ an export key
- ☐ a password
- ☐ a user certificate

Question 44

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?

- ☐ incident reports
- ☐ actions
- ☐ exceptions
- ☐ user overrides

Question 45

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?

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

Question 46

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?

- ☐ Yes
- ☐ No

Question 47

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?

- ☐ eDiscovery Manager from the Security & Compliance admin center
- ☐ compliance management from the Exchange admin center
- ☐ User management administrator from the Microsoft 365 admin center
- ☐ Information Protection administrator from the Azure Active Directory admin center

Question 48

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?

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

Question 49

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?

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

Question 50

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E3 license.

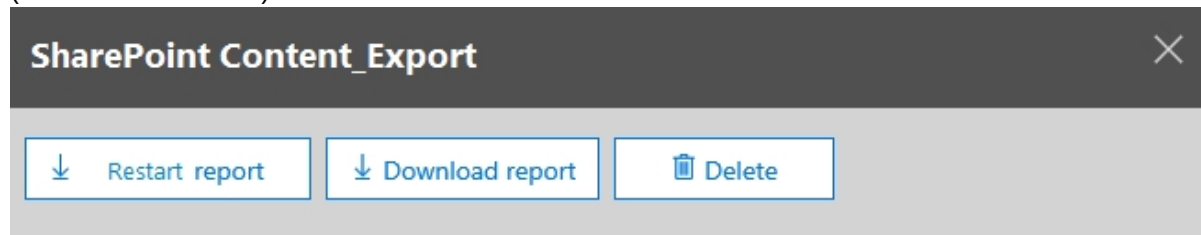
You enable auditing for your organization.

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

- ☐ 2 years
- ☐ 1 year
- ☐ 30 days
- ☐ 90 days

Question 51

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

**Status:**

The export has completed. You can start downloading the results.

Items included from the search:

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:

One PST file for each mailbox.

De-duplication for Exchange content:

Not enabled.

SharePoint document versions:

Included

Export files in a compressed (zipped) folder:

Yes

The export data was prepared within region:

Default region

Close

Feedback

What will be excluded from the export?

- ☐ a 60-MB DOCX file
- ☐ a 5-MB MP3 file
- ☐ a 10-MB XLSX file
- ☐ a 5-KB RTF file
- ☐ an 80-MB PPTX file
- ☐ a 100-MB VSDX file

Question 52

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?

- ☐ Yes
- ☐ No

Question 53

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?

- ☐ the locations of the DLP policy
- ☐ the user overrides of the DLP policy rule
- ☐ the status of the DLP policy
- ☐ the conditions of the DLP policy rule

Question 54

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.

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

Question 55

HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses.

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

Six months later, a manager sends you an email message asking the following questions:

Question1: Who created a team named Team1 14 days ago?

Question2: Who signed in to the mailbox of User1 30 days ago?

Question3: Who changed the site collection administrators of a site 60 days ago?

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	☐	☐
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	☐	☐
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	☐	☐

Case Study (3 questions)

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 shown 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 uses. 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 56

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

What should you create?

- ☐ a data loss prevention (DLP) policy from the Security & Compliance admin center
- ☐ a data loss prevention (DLP) policy from the Exchange admin center
- ☐ a retention policy from the Exchange admin center
- ☐ a retention policy from the Security & Compliance admin center

Question 57

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.

Actions	Answer Area
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.	

Question 58

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

What should you create?

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