- **Vendor: Microsoft**
- **Exam Code: MS-101**
- **Exam Name: Microsoft 365 Mobility and Security**
- **New Updated Questions from Braindump2go (Updated in June/2020)**

QUESTION 106
Hotspot Question
You create two device compliance policies for Android devices as shown in the following table.

Name	Member of	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	*None*
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft Intune.
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
The device of User1 is compliant.	○	○
The device of User2 is compliant.	○	○
The device of User3 is compliant.	○	○

Answer:

Answer Area

Statements	Yes	No
The device of User1 is compliant.	○	○
The device of User2 is compliant.	○	○
The device of User3 is compliant.	○	○

Explanation:
https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android

QUESTION 107
Hotspot Question
Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.
You update the Windows 10 devices by using Windows Update for Business.
What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Quality updates: ▼
- 14 days
- 30 days
- 60 days
- 120 days

Feature updates: ▼
- 60 days
- 180 days
- 365 days
- 540 days

Answer:

Answer Area

Quality updates: ▼
- 14 days
- **30 days**
- 60 days
- 120 days

Feature updates: ▼
- 60 days
- 180 days
- **365 days**
- 540 days

Explanation:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

QUESTION 108
Hotspot Question

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.

Answer:

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.

Explanation:
https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

QUESTION 109
Hotspot Question
You have three devices enrolled in Microsoft Intune as shown in the following table.

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

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

Answer:

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

QUESTION 110
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

Answer: A
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 111
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

Answer: B
Explanation:
https://docs.microsoft.com/en-us/intune/mdm-authority-set

QUESTION 112
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.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/integrate-wd-atp

QUESTION 113
Case Study 1 - Contoso, Ltd
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 ES subscription.
Existing Environment
Requirement
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 are 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	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

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 automaticaiy.
- 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.

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

Answer: B

Explanation:

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

QUESTION 114

Case Study 1 - Contoso, Ltd

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 ES subscription.

Existing Environment

Requirement

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 are 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	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

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 automaticaiy.
- 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.

You need to create the Microsoft Store for Business.

Which user can create the store?

User2

User3

User4

User5

Answer: C
Explanation:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

QUESTION 115
Your network contains an Active Directory forest named contoso.local.
You have a Microsoft 365 subscription.
You plan to implement a directory synchronization solution that will use password hash synchronization.
From the Microsoft 365 admin center, you verify the contoso.com domain name.
You need to prepare the environment for the planned directory synchronization solution.
What should you do first?

From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.

From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.

From the Microsoft 365 admin center, verify the contoso.local domain name.

From Active Directory Users and Computers, modify the UPN suffix for all users.

Answer: B

QUESTION 116
You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. The tenant includes a user named User1.
You enable Azure AD Identity Protection.
You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.
To which role should you add User1?

Security reader

Compliance administrator

Reports reader

Global administrator

Answer: A