MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

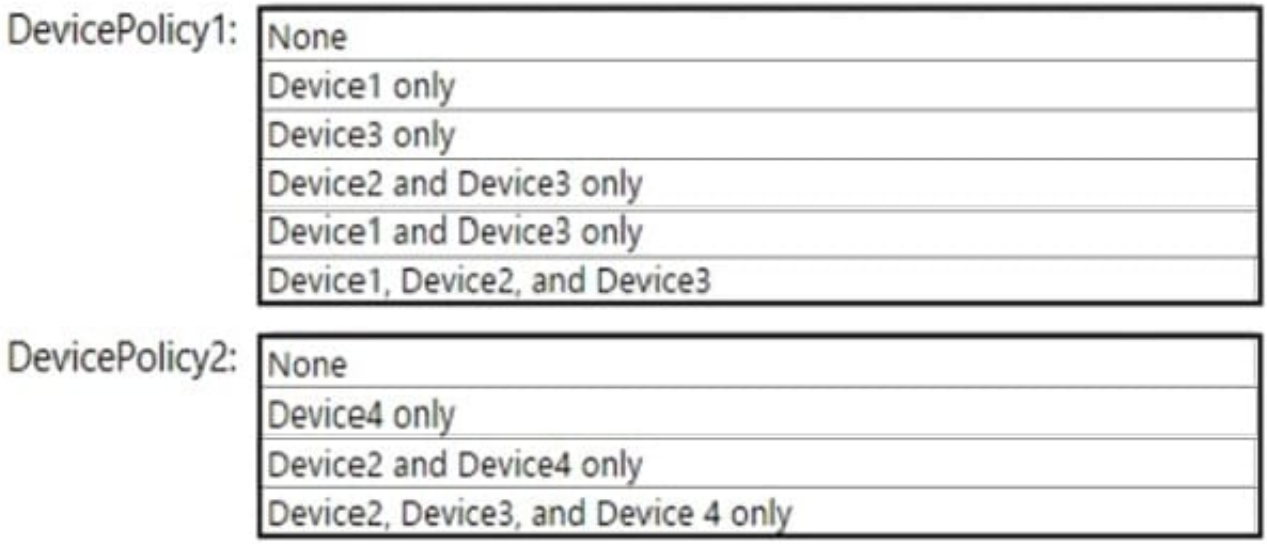
QUESTION 1

HOTSPOT

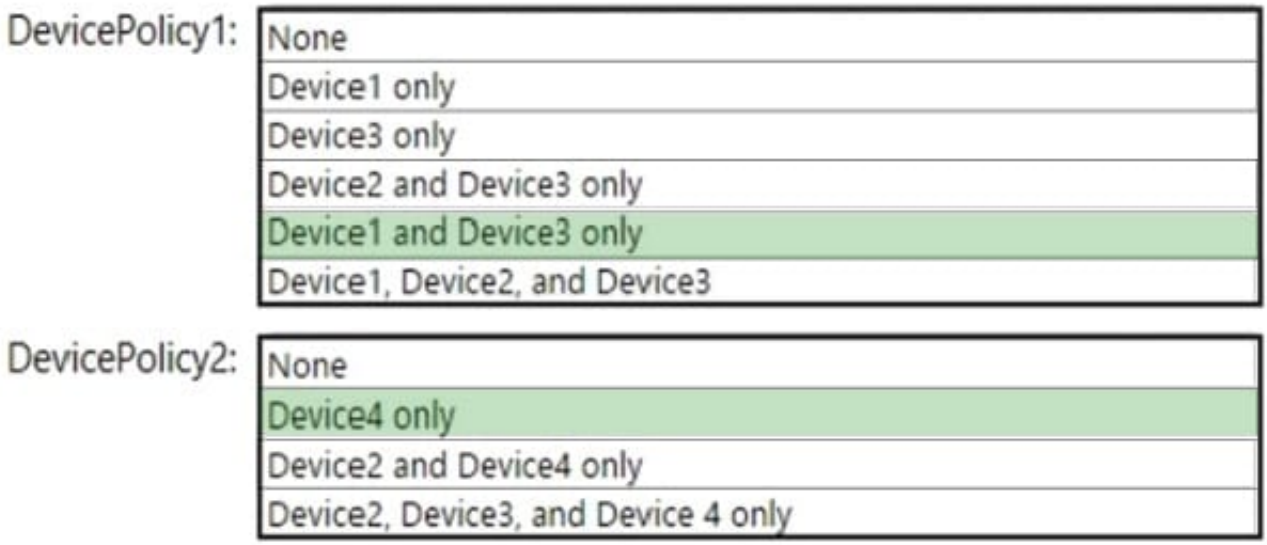
Which policies apply to which devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

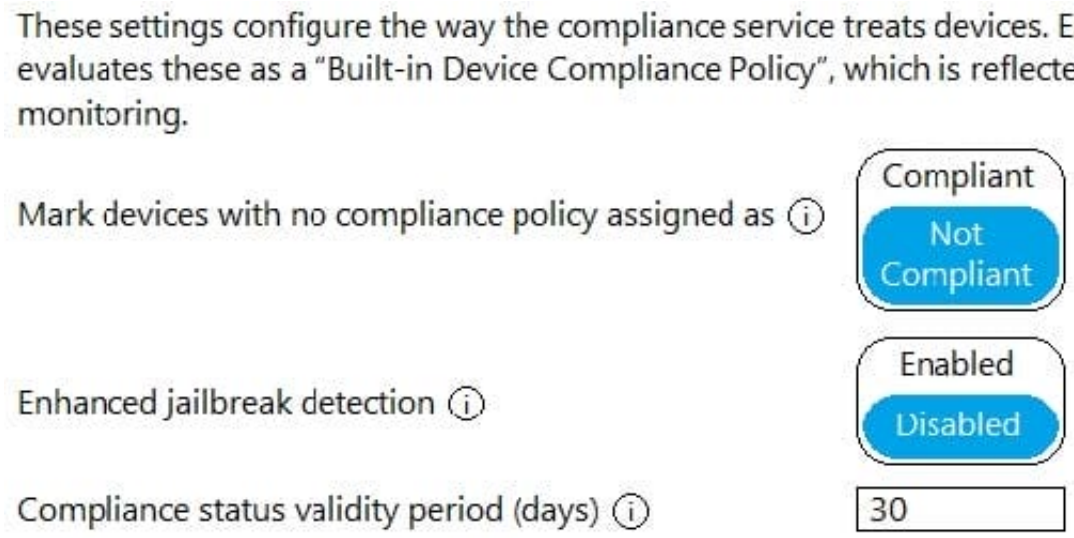


QUESTION 2

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager.

The Compliance policy settings are configured as shown in the following exhibit.



On February 25, 2020, you create the device compliance policies shown in the following table.

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Box 1: Yes

Device2 is in Group2 so Policy2 applies.

Device2 is not compliant with Policy2. However, the device won\\'t be marked as non-compliant until 10 days after the device was enrolled.

Box 2: Yes

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2. However, the device won\\'t be marked as non-

compliant until 10 days after the device was enrolled.

Box 3: No

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2.

March 12th is more than 10 days after the device was enrolled so it will now be marked as non-compliant by Policy2.

QUESTION 3

You need to create a retention policy that contains a data label. The policy must delete all Microsoft Office 365 content that is older than six months.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

Creating Office 356 labels is a two-step process. The first step is to create the actual label which includes the name, description, retention policy, and classifying the content as a record. Once this is completed, the second step requires the deployment of a label using a labelling policy which specifies the specific location to publish and applying the label automatically.

To create an Office 365 label, following these steps:

1.

Open Security and Compliance Centre;

2.

Click on Classifications;

3.

Click on Labels;

4.

The label will require configuration including: name your label (Name), add a description for the admins (Description for Admins), add a description for the users (Description for Users);

5.

Click Next once the configuration is completed;

6.

Click Label Settings on the left-hand side menu;

7.

The Label Settings will need to be configured. On this screen, you can toggle the Retention switch to either “on” or “off”. If you choose “on”, then you can answer the question “When this label is applied to content” with one of two

options. The first option is to Retain the Content. From the pick boxes, you can choose the length of retention and upon the end of the retention, the action that will take place. The three actions are to delete the data, trigger an approval flow for review, or nothing can be actioned. The second option is to not retain the data after a specified amount of time or based on the age of the data; and

8.

The label has now been created.

To create a label policy, follow these steps:

1.

Open Security and Compliance Centre;

2.

Click on Data Governance, Retention;

3.

Choose Label Policies box at the top of the screen; and

4.

There are now two options. The first is to Publish Labels. If your organization wants its end users to apply the label manually, then this is the option you would choose. Note that this is location based. The second option is to Auto-apply Labels. With Auto-apply, you would have the ability to automatically apply a label when it meets the specified criteria.

References: https://www.maadarani.com/office-365-classification-and-retention-labels/

QUESTION 4

You have a Microsoft 365 subscription.

Your company uses Jamf Pro to manage macOS devices.

You plan to create device compliance policies for the macOS devices based on the Jamf Pro data.

You need to connect Microsoft Endpoint Manager to Jamf Pro.

What should you do first?

A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.

B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.

C. From the Endpoint Management admin center, configure Partner device management.

D. From the Azure Active Directory admin center, register an application.

Correct Answer: D

Connect Intune to Jamf Pro (To connect Intune with Jamf Pro steps are):

1.

Create a new application in Azure. (In the Azure portal, go to Azure Active Directory > App Registrations, and then select New registration.)

2.

Enable Intune to integrate with Jamf Pro. (From MEM admin center, Select Tenant administration > Connectors and tokens > Partner device management... Enable the Compliance Connector for Jamf by pasting the Application ID you

saved during the previous procedure into the Specify the Azure Active Directory App ID for Jamf field).

3.

Configure Conditional Access in Jamf Pro.

Step a. Activate the connection in the Jamf Pro console: Open the Jamf Pro console and navigate to Global Management > Conditional Access. Click the Edit button on the macOS Intune Integration tab.

Step b. In Intune, go to the Partner device management page. Under Connector Settings configure groups for assignment

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf

QUESTION 5

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to install Azure AD Connect and enable single sign-on (SSO).

You need to prepare the domain to support SSO. The solution must minimize administrative effort.

What should you do?

A. Raise the forest functional level to Windows Server 2016.

B. Modify the UPN suffix of all domain users.

C. Populate the mail attribute of all domain users.

D. Rename the domain.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide