MS-101 Q&As

Microsoft 365 Mobility and Security

Pass Microsoft MS-101 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ms-101.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

A. an app configuration policy

B. an app

C. a device configuration profile

D. a device compliance policy

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

QUESTION 2

You plan to use Microsoft Sentinel and Microsoft Defender for Cloud Apps.

You need to connect Microsoft Defender for Cloud Apps to Microsoft Sentinel.

What should you do in the Microsoft Defender for Cloud Apps portal?

A. From Automatic log upload, add a data source.

B. From Automatic log upload, add a log collector.

C. From Connected apps, add an app connector.

D. From Security extensions, add a SIEM agent.

Correct Answer: D

Explanation:

Integrating with Microsoft Sentinel

In the Defender for Cloud Apps portal, under the Settings cog, select Security extensions.

On the SIEM agents tab, select add (+), and then choose Microsoft Sentinel.

In the wizard, select the data types you want to forward to Microsoft Sentinel. Etc

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/siem-sentinel

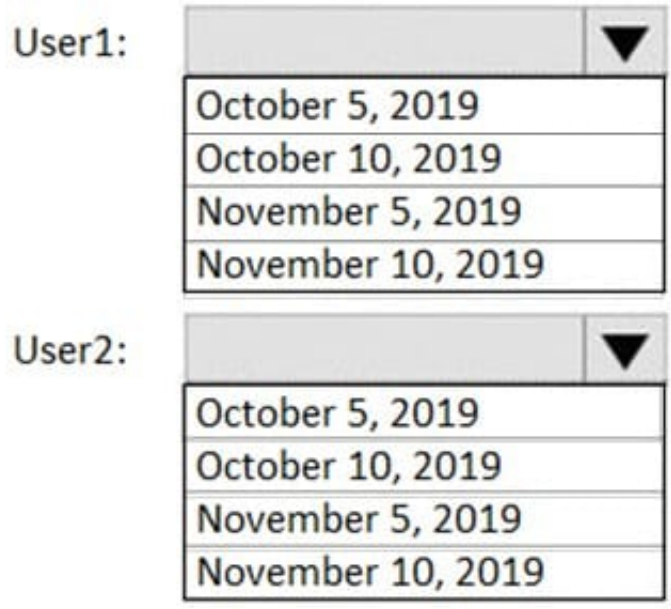
QUESTION 3

HOTSPOT

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

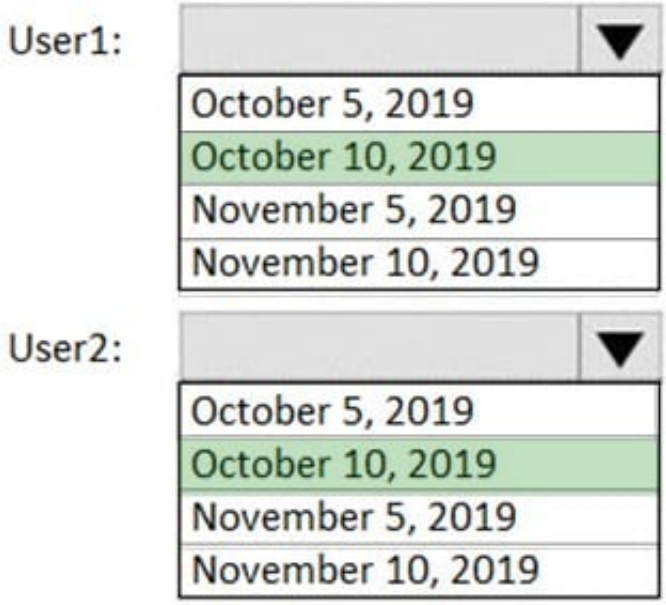
The devices onboarded to Microsoft Defender ATP are shown in the following table.

Answer Area



The alerts visible in the Microsoft Defender ATP alerts queue are shown in the following table.

Answer Area



You create a suppression rule that has the following settings:

1.

Triggering IOC: Any IOC

2.

Action: Hide alert

3.

Suppression scope: Alerts on ATP1 machine group

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

NOTE: Each correct selection is worth one point.

Hot Area:

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

Correct Answer:

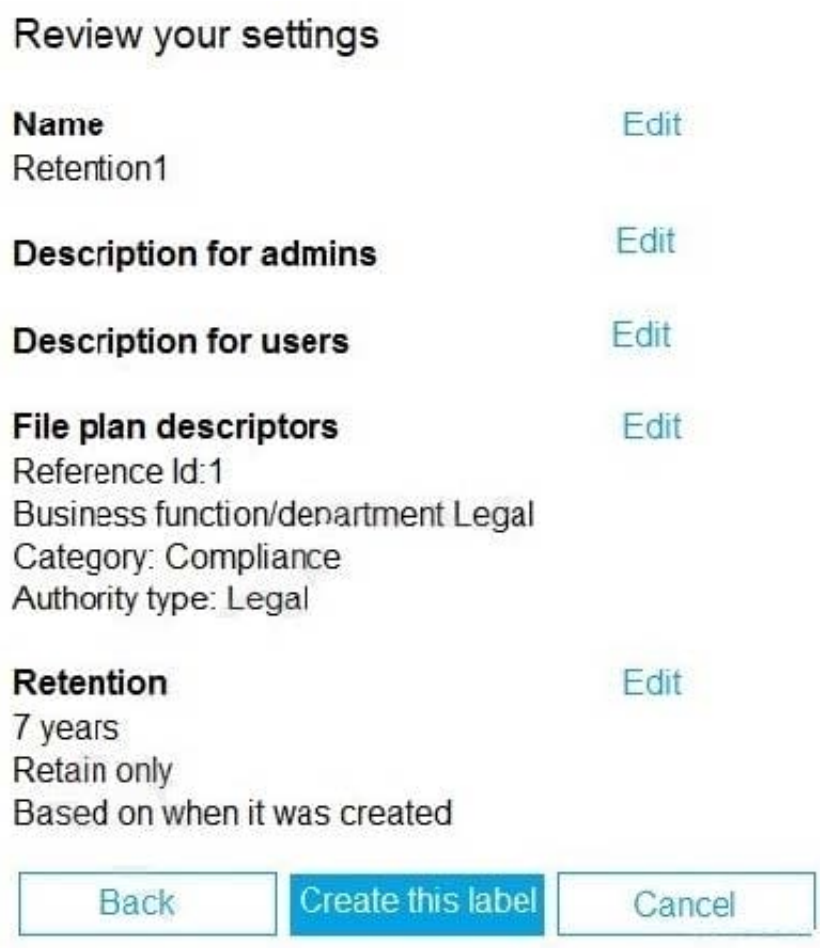
Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

QUESTION 4

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.



When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

A. Create a new label policy

B. Modify the Authority type setting for Retention!

C. Modify the Business function/department setting for Retention 1.

D. Use a file plan CSV template to import Retention1.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

QUESTION 5

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

Latest MS-101 Dumps MS-101 PDF Dumps MS-101 Practice Test