MD-101 Q&As

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

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

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

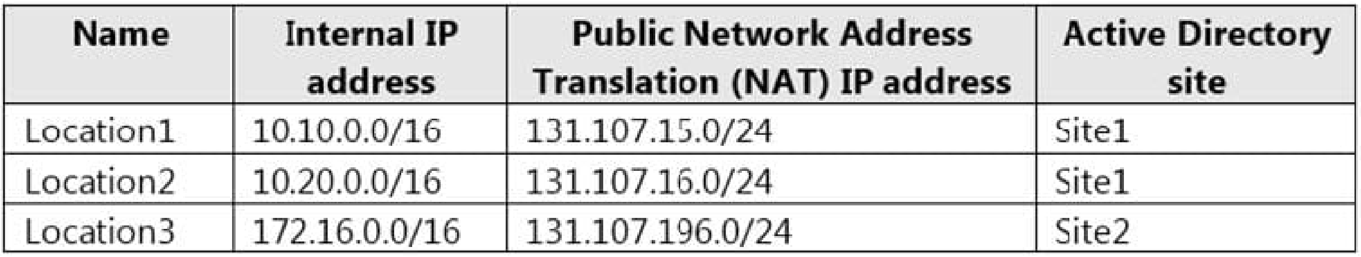
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

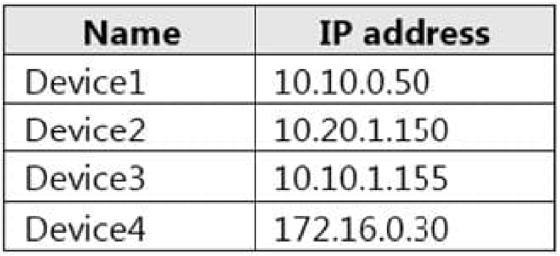
HOTSPOT

Your network contains an on-premises Active Directory domain that contains the locations shown in the following table.

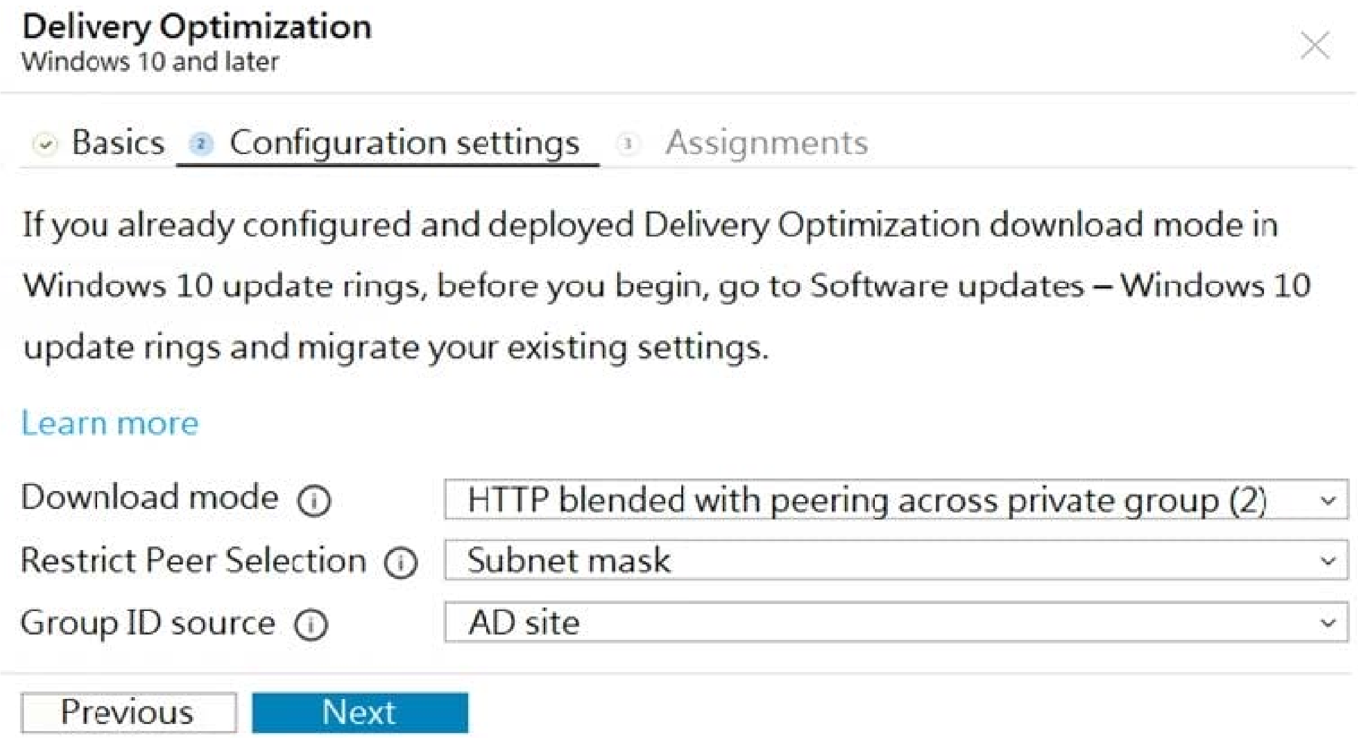


Name	Internal IP address	Public Network Address Translation (NAT) IP address	Active Directory site
Location1	10.10.0.0/16	131.107.15.0/24	Site1
Location2	10.20.0.0/16	131.107.16.0/24	Site1
Location3	172.16.0.0/16	131.107.196.0/24	Site2

In Microsoft Intune, you enroll the Windows 10 devices shown in the following table. You have a Delivery Optimization device configuration profile applied to all the devices. The profile is configured as shown in the following exhibit.



Name	IP address
Device1	10.10.0.50
Device2	10.20.1.150
Device3	10.10.1.155
Device4	172.16.0.30



Delivery Optimization
Windows 10 and later

If you already configured and deployed Delivery Optimization download mode in Windows 10 update rings, before you begin, go to Software updates – Windows 10 update rings and migrate your existing settings.

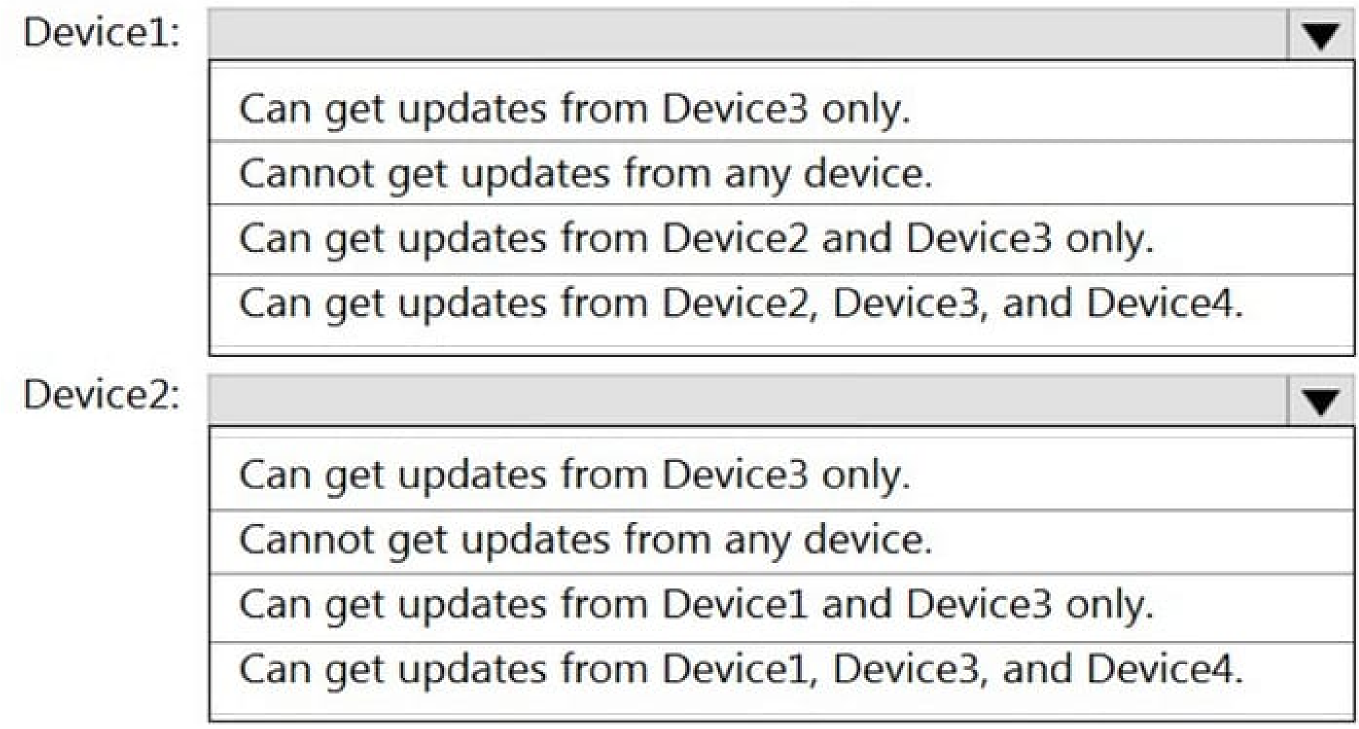
Learn more

Download mode: HTTP blended with peering across private group (2)
Restrict Peer Selection: Subnet mask
Group ID source: AD site

From which devices can Device1 and Device2 get updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



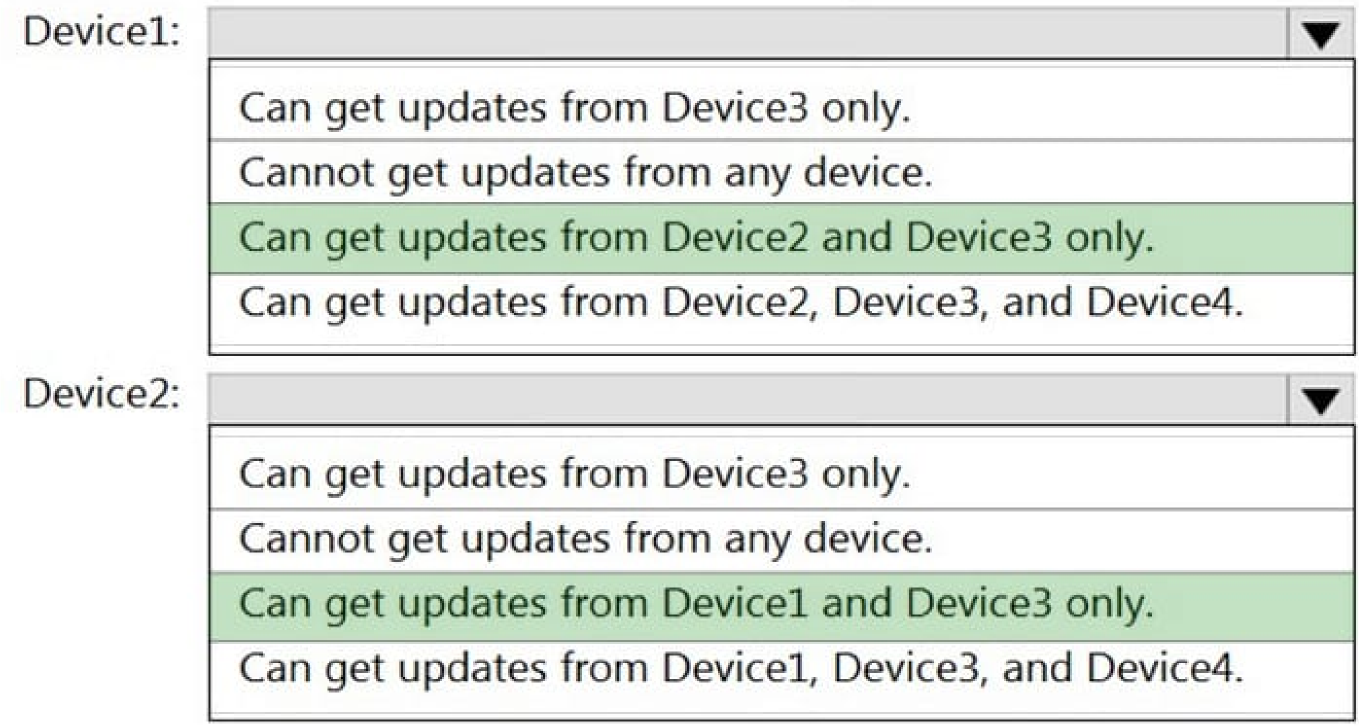
Device1:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device2 and Device3 only.
- Can get updates from Device2, Device3, and Device4.

Device2:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device1 and Device3 only.
- Can get updates from Device1, Device3, and Device4.

Correct Answer:



Device1:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- [✓ Can get updates from Device2 and Device3 only.]
- Can get updates from Device2, Device3, and Device4.

Device2:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- [✓ Can get updates from Device1 and Device3 only.]
- Can get updates from Device1, Device3, and Device4.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference#select-the-source-of-group-ids

QUESTION 2

All users at your company have Azure AD joined Windows 10 workstations that are managed via Microsoft Intune.

You have been tasked with making sure that Windows Analytics is used to monitor the workstations centrally.

Which of the following actions should you take?

A. You should create a device configuration profile via Intune.

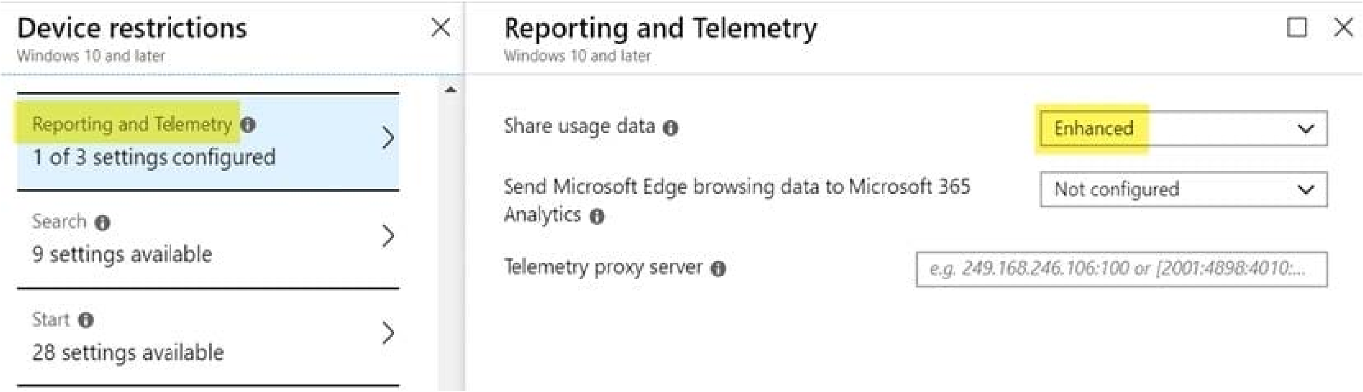
B. You should create a device compliance policy via Intune.

C. You should create a Windows AutoPilot deployment profile via Intune.

D. You should create an app configuration policy via Intune.

Correct Answer: A

With Intune, use Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. Configure Delivery Optimization as part of your device configuration profiles.



Device restrictions
Windows 10 and later

Reporting and Telemetry
1 of 3 settings configured

Search
9 settings available

Start
28 settings available

Reporting and Telemetry
Windows 10 and later

Share usage data: Enhanced

Send Microsoft Edge browsing data to Microsoft 365 Analytics: Not configured

Telemetry proxy server: e.g. 249.168.246.106:100 or [2001:4898:4010:...

Reference: https://www.scconfigmgr.com/2019/03/27/windows-analytics-onboarding-with-intune/

QUESTION 3

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft Intune. You are creating a device configuration profile for the workstations. You have been informed that a custom image should be displayed as the Desktop background picture. Which of the following is a Device restriction setting that should be configured?

A. Locked screen experience

B. Personalization

C. Display

D. General

Correct Answer: B

Wallpaper image, or Desktop background picture, URL is set under Personalization.

References: https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10

QUESTION 4

All of your company\\'s devices are managed via Microsoft Intune.

conditional access is used to prevent devices that are not compliant with company security policies, from accessing Microsoft 365 services.

You need to access Device compliance to view the non-compliant devices.

Where should you access Device compliance from?

A. System Center Configuration Manager

B. Windows Defender Security Center.

C. The Intune admin center.

D. The Azure Active Directory admin center.

Correct Answer: C

Open the Intune Device compliance dashboard:

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

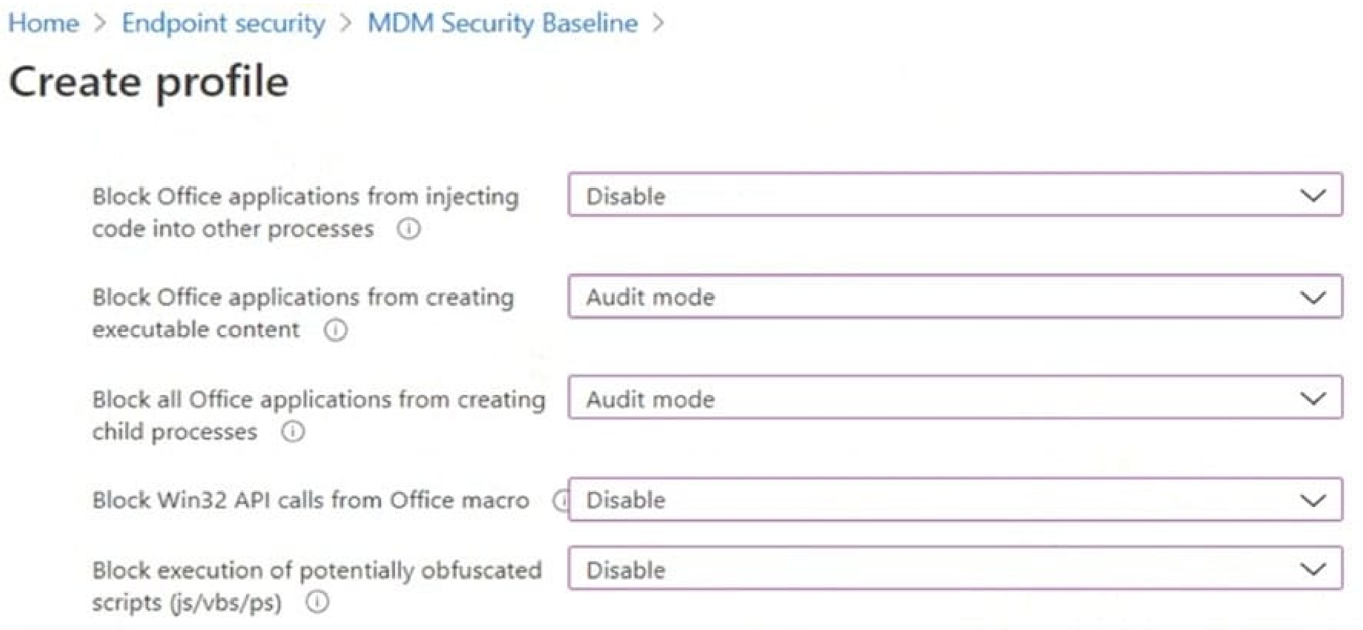
Select Devices > Overview > Compliance status tab. Important: Devices must be enrolled into Intune to receive device compliance policies. Note 1: Intune Admin portal URL, Microsoft Endpoint Manager admin center: https://endpoint.microsoft.com Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud- based mobile application management (MAM), and cloud-based PC management for your organization. Note 2: Compliance reports help you review device compliance and troubleshoot compliance-related issues in your organization. Using these reports, you can view information on: The overall compliance states of devices The compliance status for an individual setting The compliance status for an individual policy Drill down into individual devices to view specific settings and policies that affect the device

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor
https://docs.microsoft.com/en-us/mem/intune/fundamentals/account-sign-up

QUESTION 5

HOTSPOT

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)

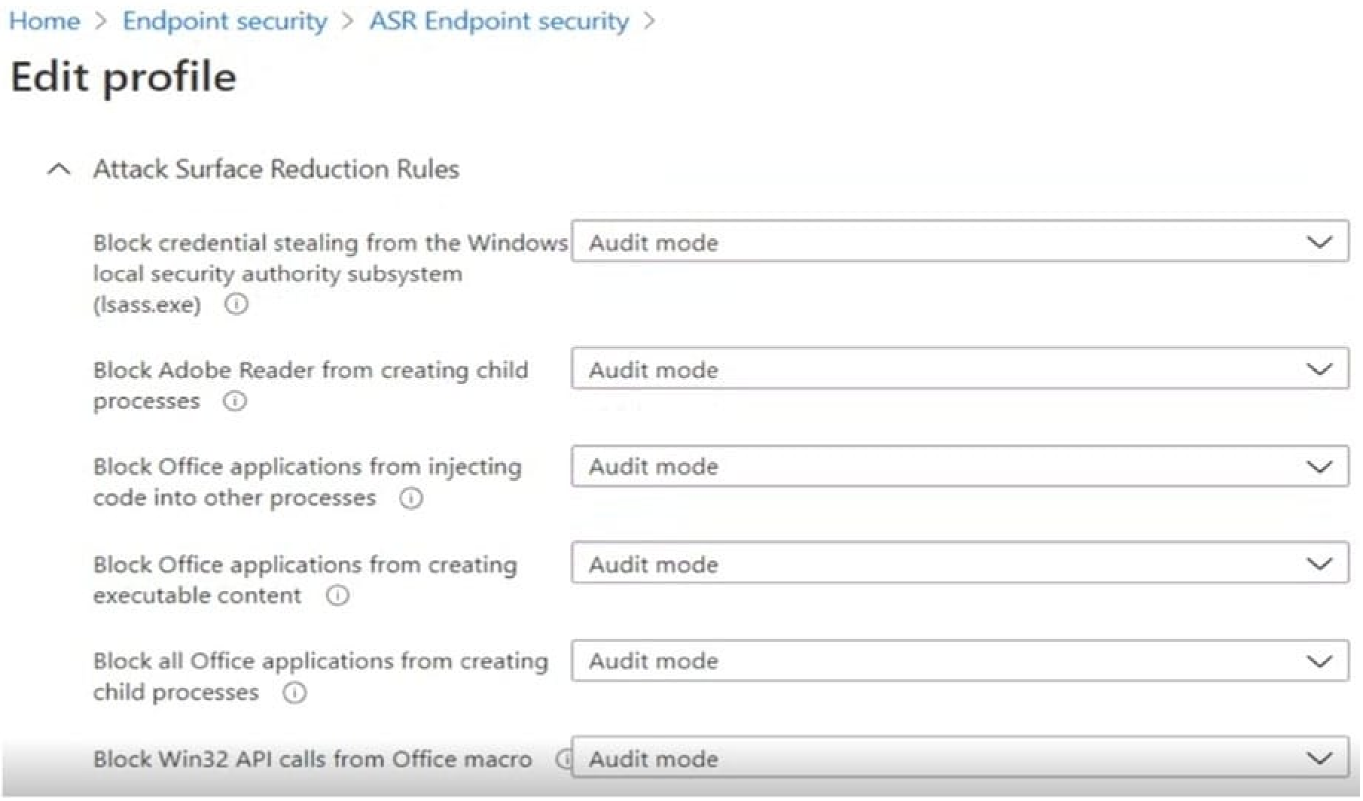


Home > Endpoint security > MDM Security Baseline >

Create profile

Block Office applications from injecting code into other processes ⓘ	Disable
Block Office applications from creating executable content ⓘ	Audit mode
Block all Office applications from creating child processes ⓘ	Audit mode
Block Win32 API calls from Office macro ⓘ	Disable
Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ	Disable

You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)



Home > Endpoint security > ASR Endpoint security >

Edit profile

Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ	Audit mode
Block Adobe Reader from creating child processes ⓘ	Audit mode
Block Office applications from injecting code into other processes ⓘ	Audit mode
Block Office applications from creating executable content ⓘ	Audit mode
Block all Office applications from creating child processes ⓘ	Audit mode
Block Win32 API calls from Office macro ⓘ	Audit mode

You plan to deploy both profiles to devices enrolled in Microsoft Intune.

You need to identify how the following settings will be configured on the devices:

1.

Block Office applications from creating executable content

2.

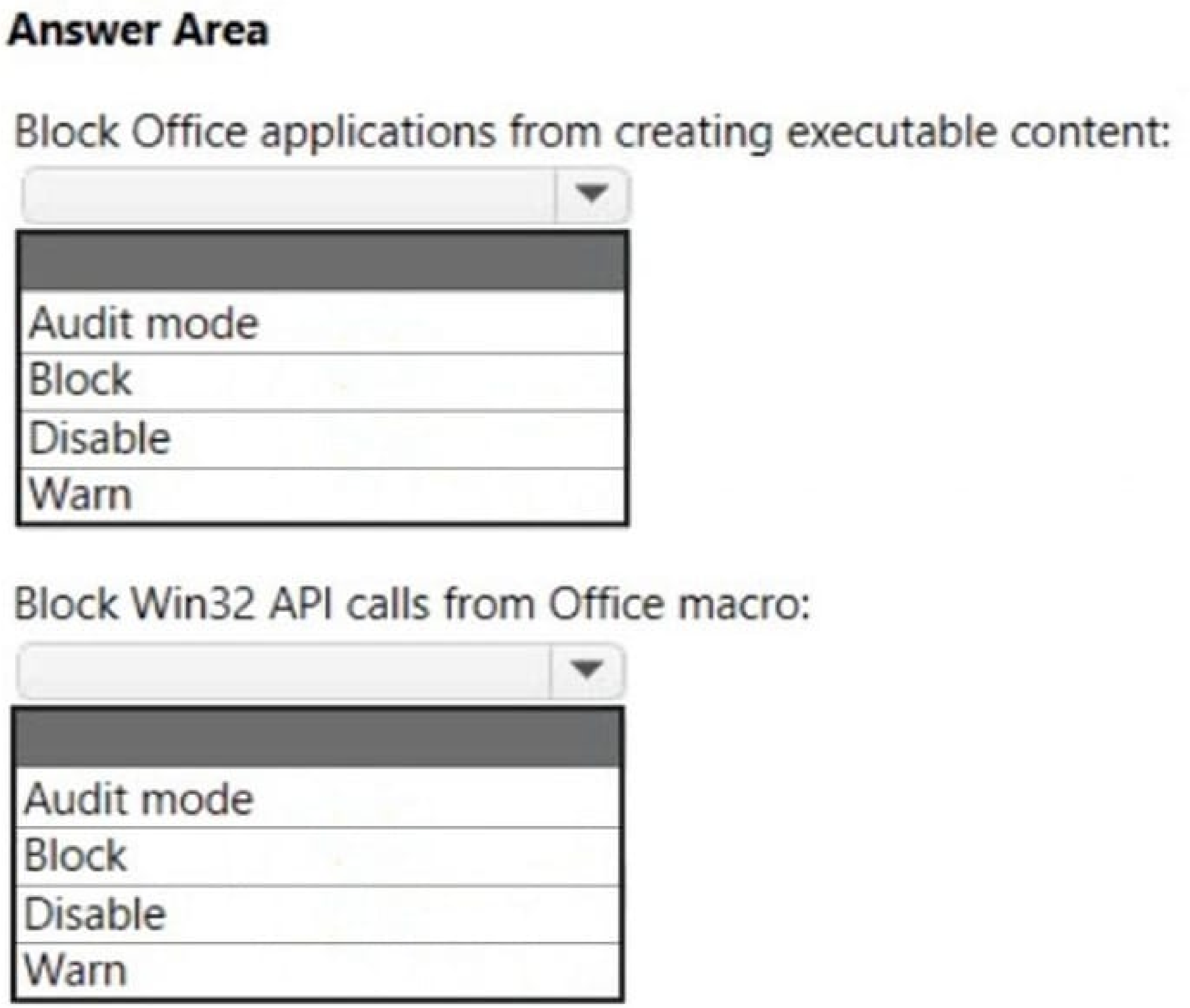
Block Win32 API calls from Office macro

Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

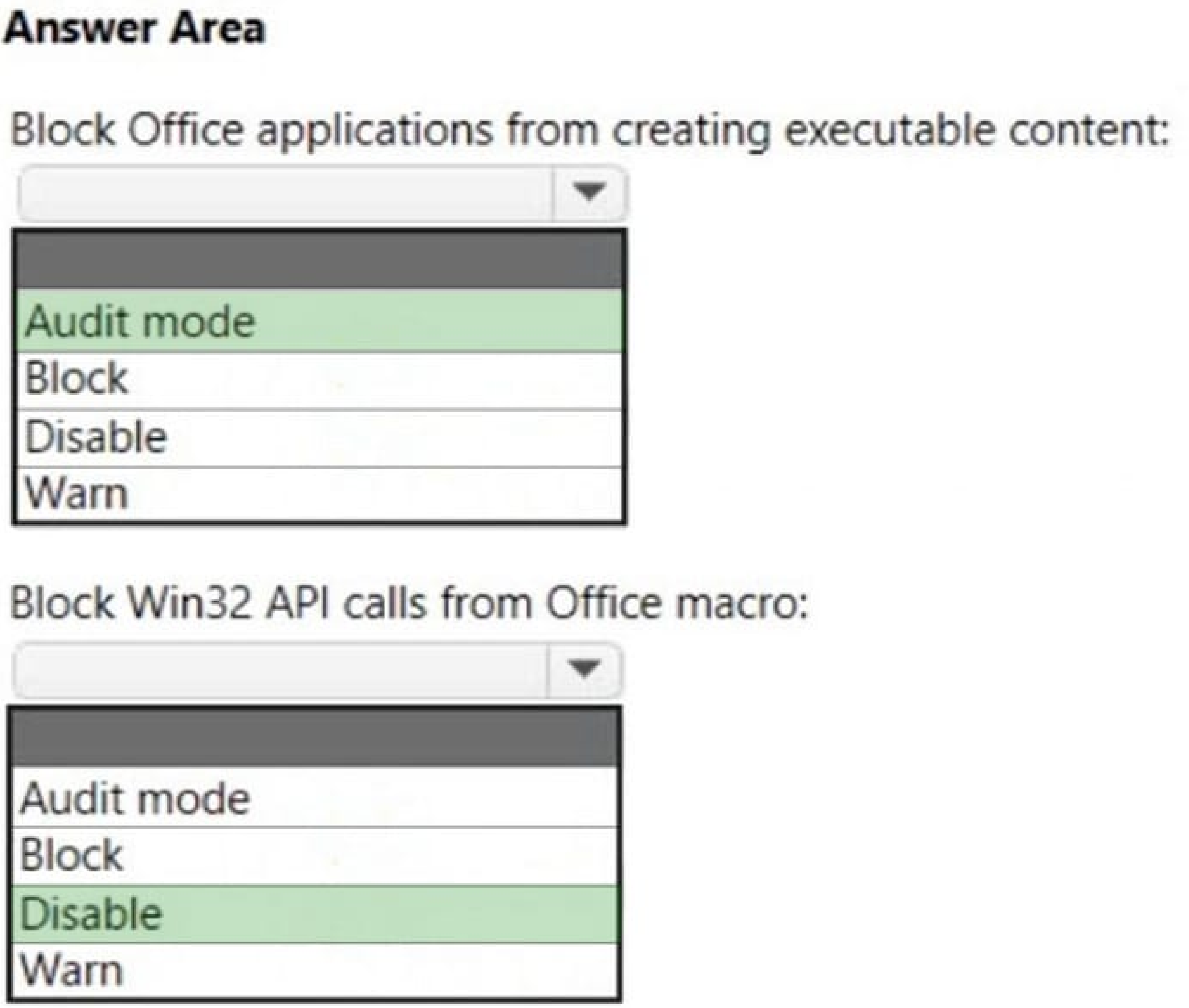


Answer Area

Block Office applications from creating executable content:

Block Win32 API calls from Office macro:

Correct Answer:



Answer Area

Block Office applications from creating executable content:

- [✓ Audit mode]
- Block
- Disable
- Warn

Block Win32 API calls from Office macro:

- Audit mode
- Block
- [✓ Disable]
- Warn

Box 1: Audit mode

According to the ASR Endpoint Security profile and to the MDM Security Baseline profile

Block Office applications from creating executable content is set to Audit mode.

Box 2: Disable

Block Win32 API calls from Office macro: According to MDM Security Baseline profile it is set to disable. According to the ASR Endpoint Security profile it is set to

Audit mode.

The profiles are merged. The Baseline profile overrides the Endpoint Security profile.

Note:

When two or more policies have conflicting settings, the conflicting settings are not added to the combined policy, while settings that don\\'t conflict are added to the superset policy that applies to a device.

Attack surface reduction rule merge behavior is as follows:

Endpoint security > Security baselines > Microsoft Defender for Endpoint Baseline > Attack Surface Reduction Rules.

MDM Security Baseline profile ASR Endpoint Security profile.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy