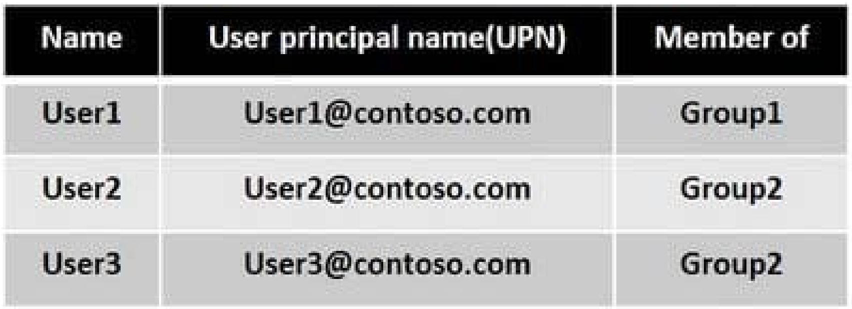
MS-500$^{Q\&As}$

Microsoft 365 Security Administration

QUESTION 1

HOTSPOT

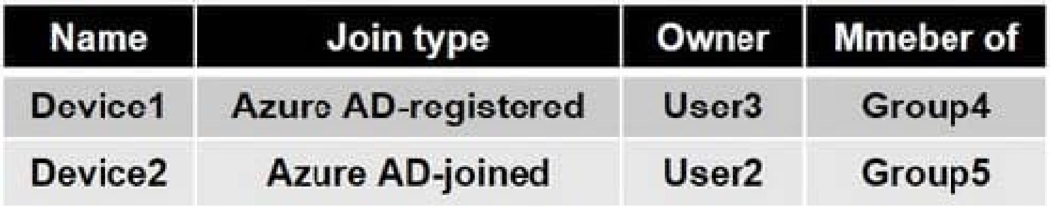
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	User principal name(UPN)	Member of
User1	User1@contoso.com	Group1
User2	User2@contoso.com	Group2
User3	User3@contoso.com	Group2

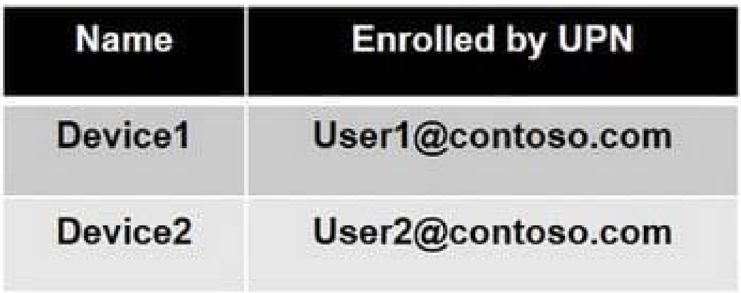
Group1 is member of a group named Group3.

The Azure Active Directory (Azure AD) tenant contains the Windows 10 devices shown in the following table.



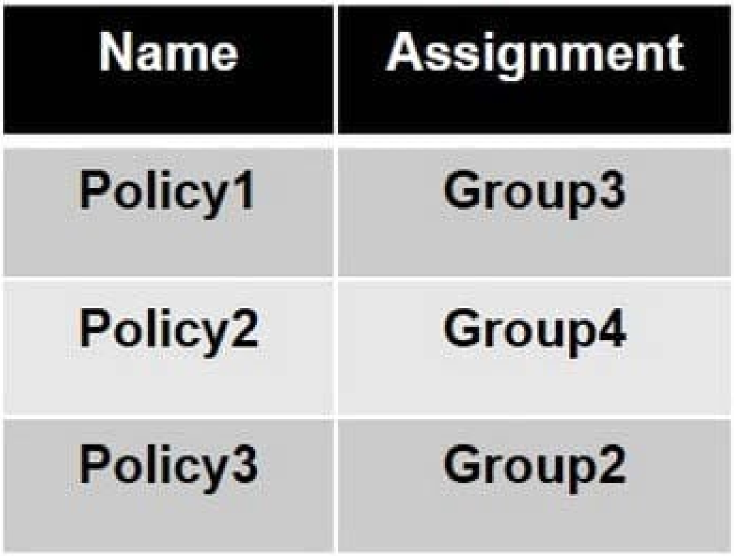
Name	Join type	Owner	Mmeber of
Device1	Azure AD-registered	User3	Group4
Device2	Azure AD-joined	User2	Group5

Microsoft Endpoint Manager has the devices shown in the following table.



Name	Enrolled by UPN
Device1	User1@contoso.com
Device2	User2@contoso.com

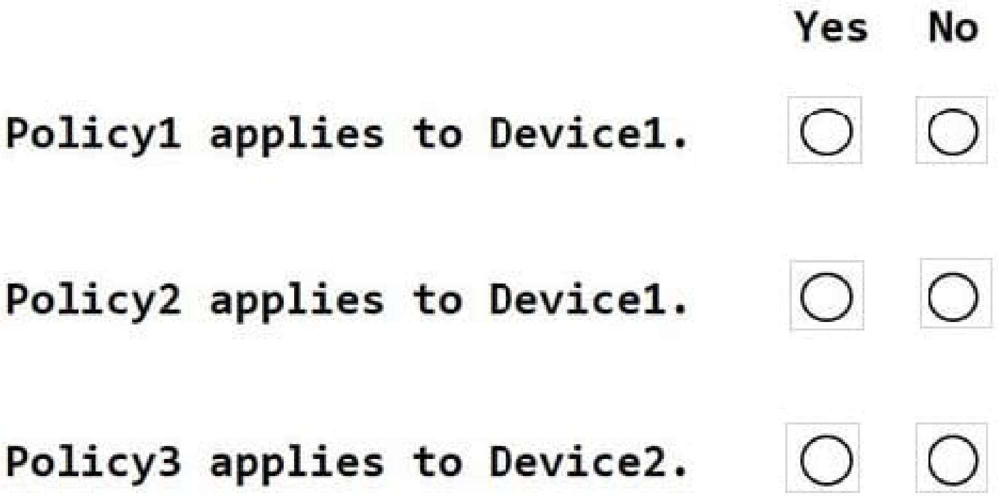
Microsoft Endpoint Manager contains the compliance policies shown in the following table.



Name	Assignment
Policy1	Group3
Policy2	Group4
Policy3	Group2

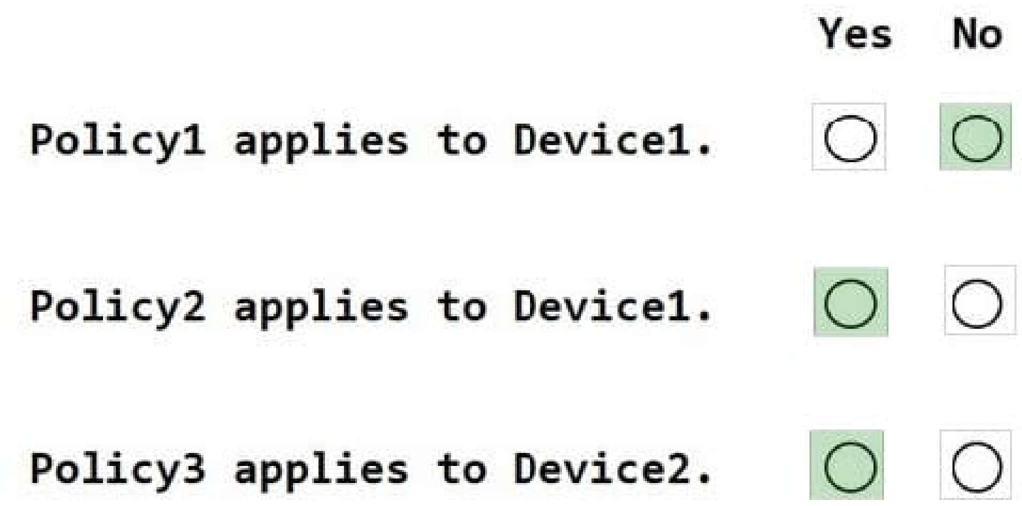
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



	Yes	No
Policy1 applies to Device1.	○	○
Policy2 applies to Device1.	○	○
Policy3 applies to Device2.	○	○

Correct Answer:



	Yes	No
Policy1 applies to Device1.	○	[✓ ○]
Policy2 applies to Device1.	[✓ ○]	○
Policy3 applies to Device2.	[✓ ○]	○

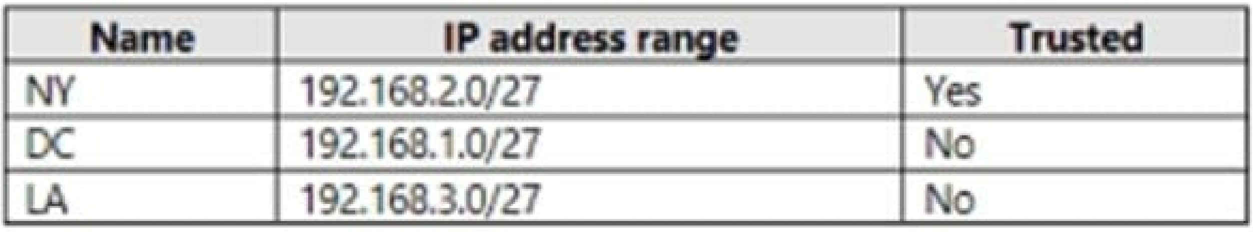
Deploy to users in user groups or devices in device groups. When a compliance policy is deployed to a user, all the user\\'s devices are checked for compliance. Using device groups in this scenario helps with compliance reporting.

QUESTION 2

HOTSPOT

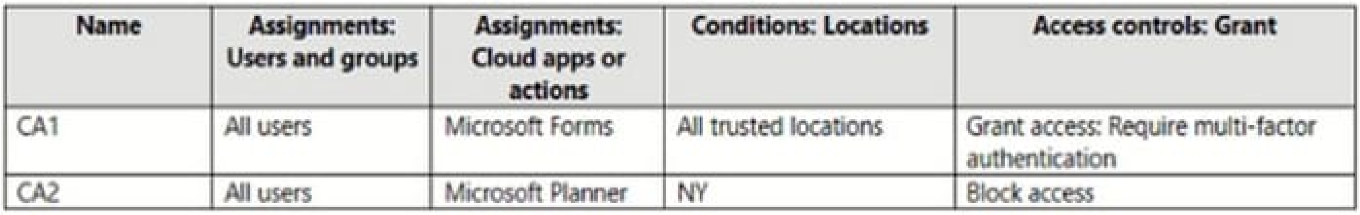
You have a Microsoft 365 subscription that contains three users named User1, User2, and User3.

You have the named locations shown in the following table.



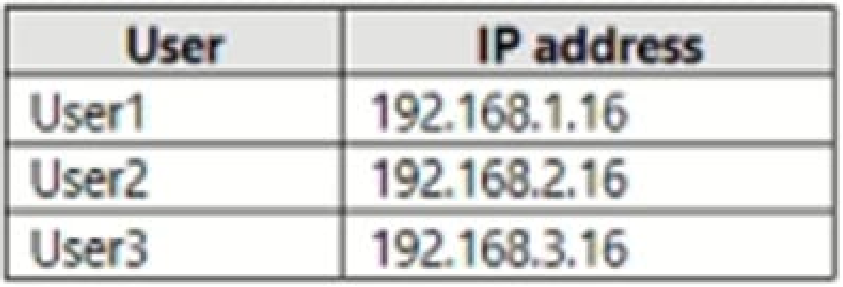
Name	IP address range	Trusted
NY	192.168.2.0/27	Yes
DC	192.168.1.0/27	No
LA	192.168.3.0/27	No

You configure an Azure Multi-Factor Authentication (MFA) trusted IP address range of 192.168.1.0/27. You have the Conditional Access policies shown in the following table.



Name	Assignments: Users and groups	Assignments: Cloud apps or actions	Conditions: Locations	Access controls: Grant
CA1	All users	Microsoft Forms	All trusted locations	Grant access: Require multi-factor authentication
CA2	All users	Microsoft Planner	NY	Block access

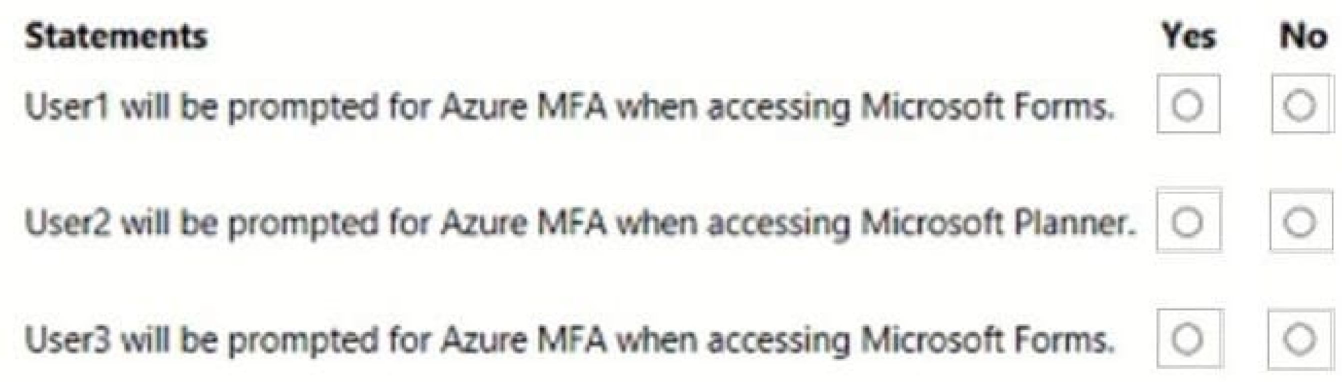
The users have the IP addresses shown in the following table.



User	IP address
User1	192.168.1.16
User2	192.168.2.16
User3	192.168.3.16

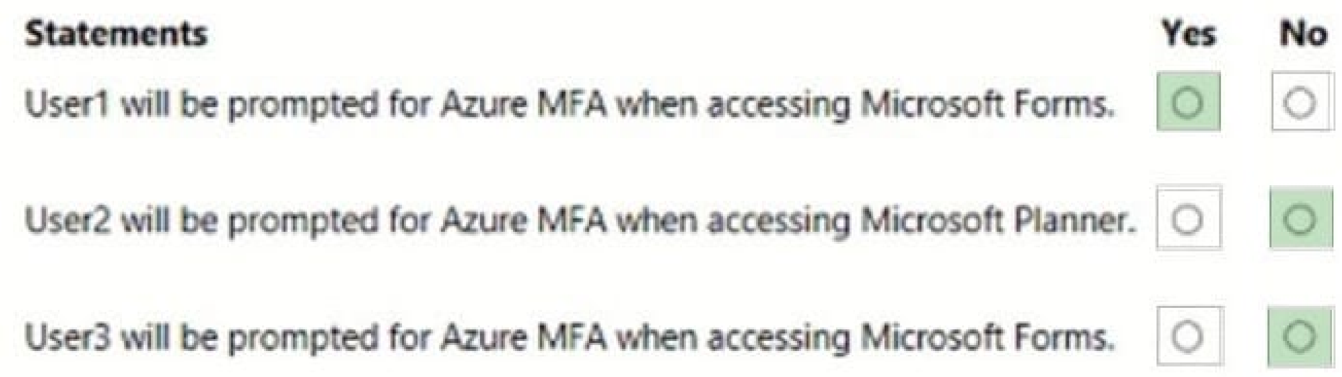
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	○
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○

Correct Answer:



Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	[✓ ○]	○
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	[✓ ○]
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	[✓ ○]

User 1 access through CA1 (forms) with Location:(included as nothing else is stated) trusted location = require MFA YES

User 2 access through CA2 (planner) with Location:(included as nothing else is stated) NY = nothing NO

User 3 access through CA1 (forms) with Location:(included as nothing else is stated) trusted location = require MFA, but NY is not a trusted location in the include, so no MFA will be promted. NO

QUESTION 3

Your company has 500 computers.

You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements:

1.

Windows Defender ATP administrators must manually approve all remediation for the executives

2.

Remediation must occur automatically for all other users

What should you recommend doing from Windows Defender Security Center?

A. Configure 20 system exclusions on automation allowed/block lists

B. Configure two alert notification rules

C. Download an offboarding package for the computers of the 20 executives

D. Create two machine groups

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups-windows-defender-advanced-threat-protection

QUESTION 4

You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP).

You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)

B. Configure Advanced Threat Protection (ATP)

C. Create a Conditional Access App Control policy for accessing Office 365

D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

QUESTION 5

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Cloud Apps enabled. You need to create an alert in Defender for Cloud Apps when source code is shared externally.

Which type of policy should you create?

A. Cloud Discovery anomaly detection

B. file

C. access

D. activity

Correct Answer: B

Detect externally shared source code

Detect when files that contain content that might be source code are shared publicly or are shared with users outside of your organization.

Prerequisites

You must have at least one app connected using app connectors.

Steps

1.

On the Policies page, create a new File policy.

2.

Select and apply the policy template Externally shared source code

3.

Optional: Customize the list of file Extensions to match your organization\\'s source code file extensions.

4.

Optional: Set the Governance actions to be taken on files when a violation is detected. The governance actions available vary between services. For example, in Box, Send policy-match digest to file owner and Put in admin quarantine.

5.

Select and apply the policy template Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/policies-information-protection#detect-externally-shared-source-code