Microsoft

AB-650

Administering Microsoft 365 and AI Services

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.1

Topic 1, Contoso Ltd

Overview
Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.
Existing Environment
Microsoft Entra configuration

Contoso has an Azure subscription.

Contoso has a Microsoft 365 E5 subscription.

Contoso has a Microsoft Entra tenant named contoso.com. The tenant has an administrative unit named AU1 that contains the following membership rule.

(device.deviceTrustType –eq "Workplace") and (device.deviceOSType –in ["Windows", "Android"])

The tenant contains the cloud-only users shown in the following table.

Name	Role	Department
Admin1	Global Administrator	Research
Admin2	AI Administrator	Research
Admin3	Privileged Role Administrator	IT
User1	• *None* • Eligible for AI Administrator	IT
User2	*None*	Development

Name	Type	Membership rule	Members
Group1	Security	*Not applicable*	User1, Group2, and Group3
Group2	Security	`(user.displayName -endsWith "1") or (user.department -eq "IT")`	*Not applicable*
Group3	Security	*Not applicable*	User2
Group4	Microsoft 365	*Not applicable*	User1 and User2

All the devices are managed by using Microsoft Intune.

Microsoft Entra authentication methods

Contoso contains an Authentication methods policy for Microsoft Authenticator that has the following settings:

Include: Group1

Exclude: Group3

Authentication mode: Passwordless

Question: 1

HOTSPOT

You need to evaluate the configuration of AU1.

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
Admin1 can add Device1 to AU1 directly.	○	○
Device2 is member of AU1.	○	○
The devices issued to Group1 will be added to AU1 automatically.	○	○

Answer:

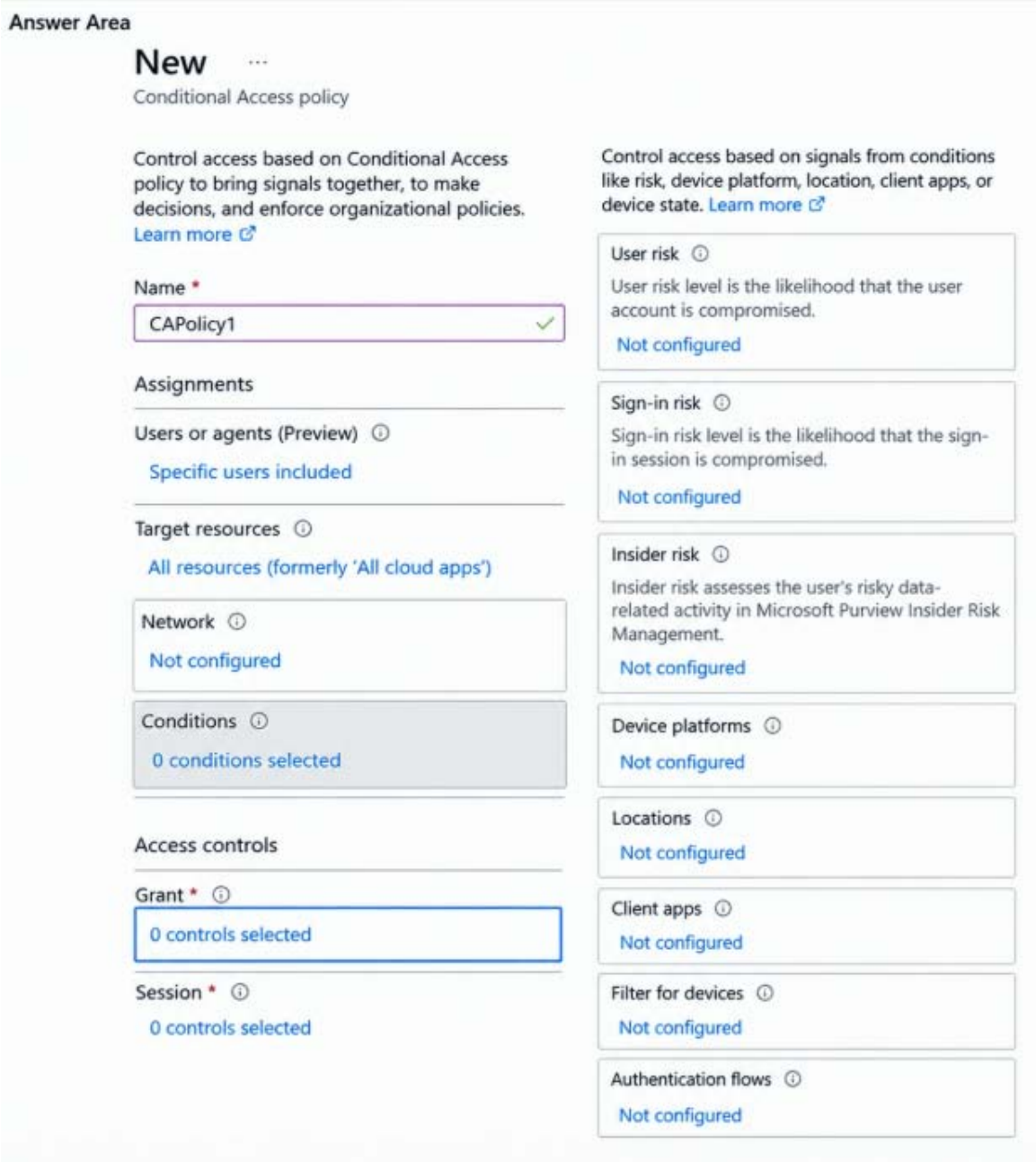
Answer Area

Statements	Yes	No
Admin1 can add Device1 to AU1 directly.	○	○
Device2 is member of AU1.	○	○
The devices issued to Group1 will be added to AU1 automatically.	○	○

Question: 2

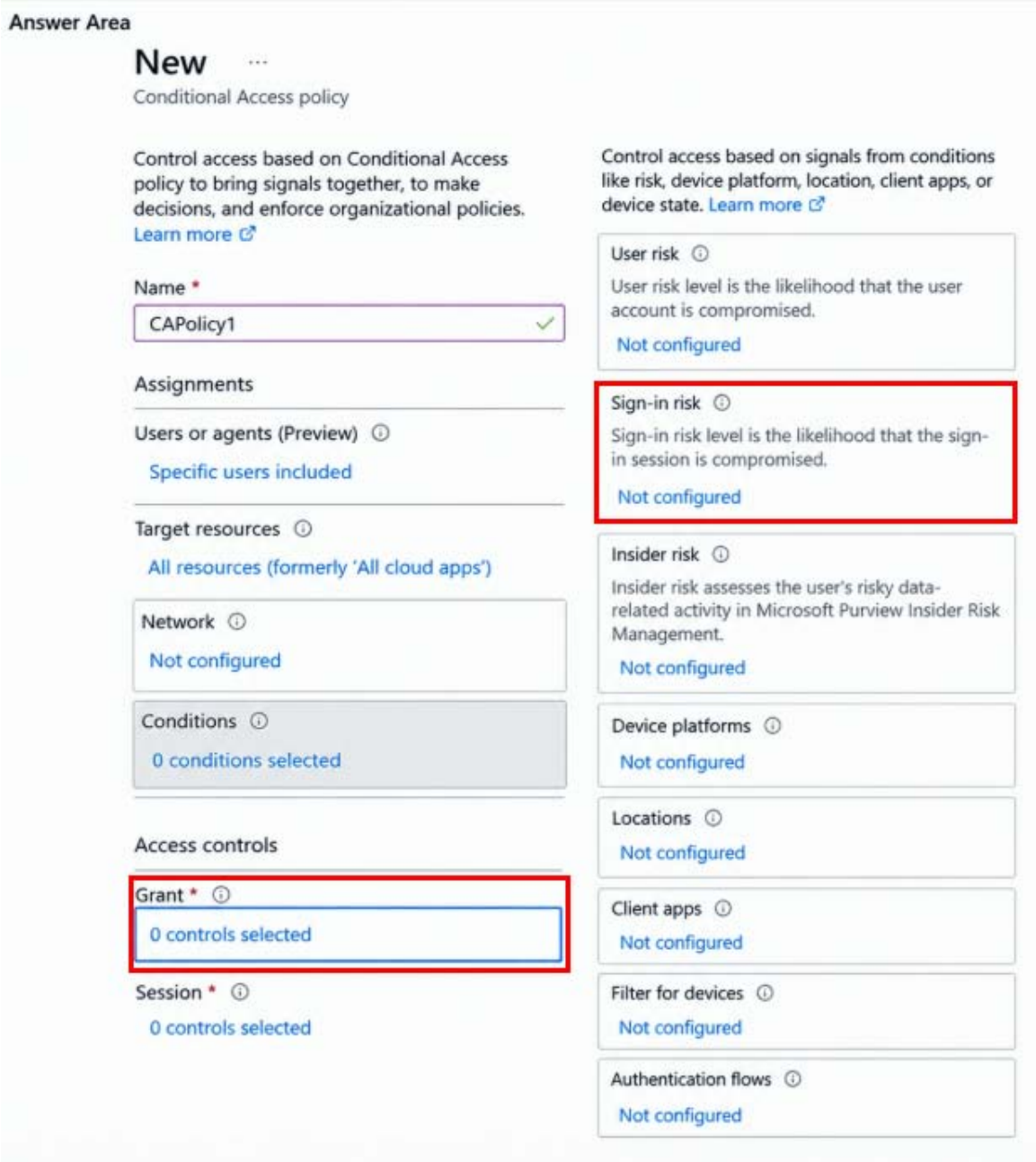
HOTSPOT

Answer Area



Answer:

Answer Area



Question: 3

You need to meet the technical requirements for the project documents.
What should you create in Microsoft Purview?

A. a sensitivity label and an auto-labeling policy
B. an Insider Risk Management policy
C. an Information Barriers policy
D. a data loss prevention (DLP) policy

Answer: D

Explanation:
Microsoft Purview Data Loss Prevention (DLP) provides controls to prevent Microsoft 365 Copilot from processing sensitive organizational content when generating responses.
Option D is correct because the Contoso technical requirement explicitly states that Microsoft 365 Copilot responses must not use content from project documents stored on SharePoint Site1.
Microsoft Purview supports a dedicated Microsoft 365 Copilot and Copilot Chat DLP policy location. Administrators can configure a DLP rule using the Content contains → Sensitivity labels condition and the Prevent Copilot from processing content action.
This prevents Copilot from processing files with the specified sensitivity labels or incorporating their contents into generated responses, even when users have SharePoint permissions.
For Contoso, the project documents can be identified using their distinctive project-code format, PR-123456789, and classified with an appropriate sensitivity label. The DLP policy can then exclude those labeled documents from Copilot processing.
Option A is incorrect as a complete solution because sensitivity labels and auto-labeling policies classify and protect documents but do not independently enforce the required Copilot processing restriction.
Option B is incorrect because Insider Risk Management detects potentially risky user activities.
Option C is incorrect because Information Barriers restrict communication and collaboration between designated user segments.
Technical consideration: The DLP policy requires an appropriate sensitivity label to be applied to the project documents. DLP rules for Copilot cannot directly exclude stored files merely by matching their project-code pattern.
Therefore, a DLP policy is the required enforcement mechanism.

Topic 2, Mix Questions

Mix Questions
Mix Questions IN THIS CASE STUDY

Question: 4

You have a Microsoft 365 subscription.

Your company has two office branches in the same city. Both branches contain Windows devices that have Windows location services disabled by policy. Each branch uses a distinct IPv4 LAN subnet.

You plan to review Microsoft 365 network connectivity insights for each branch separately.

You need to configure network connectivity to ensure that assessment results are associated with the correct branch.

What should you do?

A. Run the Microsoft 365 network connectivity test from each branch without adding the branch locations.
B. Add public egress IP address ranges for each branch without specifying the LAN subnet ranges.
C. On the Locations tab, add each branch, and then specify the LAN subnet ranges for each branch.
D. From the Network connectivity page, enable Windows location services, and then use the discovered locations.

Answer: C

Explanation:

Microsoft 365 network connectivity insights help administrators evaluate how network configuration affects connectivity to Microsoft 365 services. Accurate office-location identification is essential for associating connectivity measurements with the appropriate branch.
Option C is correct because Microsoft 365 allows administrators to define office locations manually and associate each location with its corresponding local area network subnet ranges. This configuration is particularly important when multiple branches exist in the same city. Because the branches have distinct IPv4 LAN subnets, Microsoft 365 can distinguish their connectivity measurements by using the configured subnet information.
Microsoft Learn explicitly supports the manual location configuration method when Windows Location Services is unavailable. Administrators can navigate to the Microsoft 365 admin center, access Network connectivity, and configure office locations with their respective LAN subnet information.
Option A is insufficient because simply running network tests does not establish the required persistent branch-specific subnet mapping.
Option B does not provide the local subnet information needed to distinguish branches reliably.
Option D conflicts with the stated requirement because Windows Location Services is disabled by policy. Furthermore, automatic geographic location discovery may not distinguish multiple offices in the same city.
Therefore, manually configuring both locations and their LAN subnet ranges meets the requirement.
Microsoft Reference:

https://learn.microsoft.com/en-us/Microsoft-365/Enterprise/office-365-network-mac-perf-overview?view=o365-worldwide

Question: 5

HOTSPOT

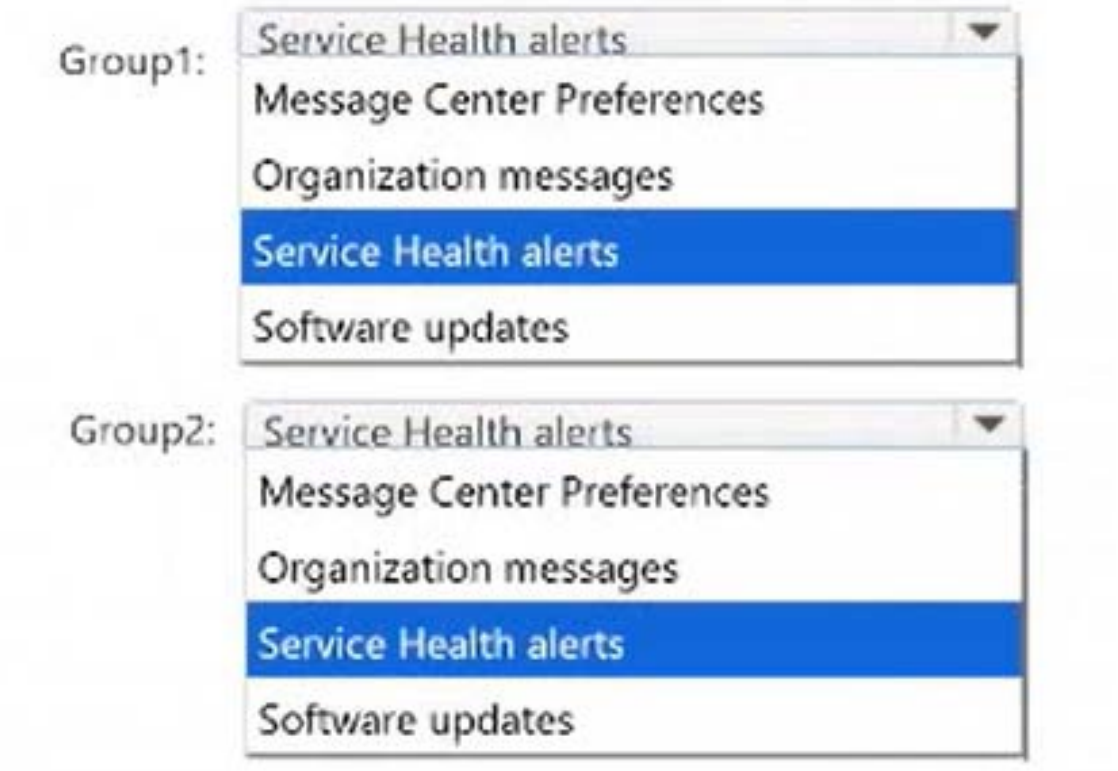
You have a Microsoft 365 subscription that contains two groups named Group1 and Group2.

You need to configure tenant notifications to meet the following requirements.

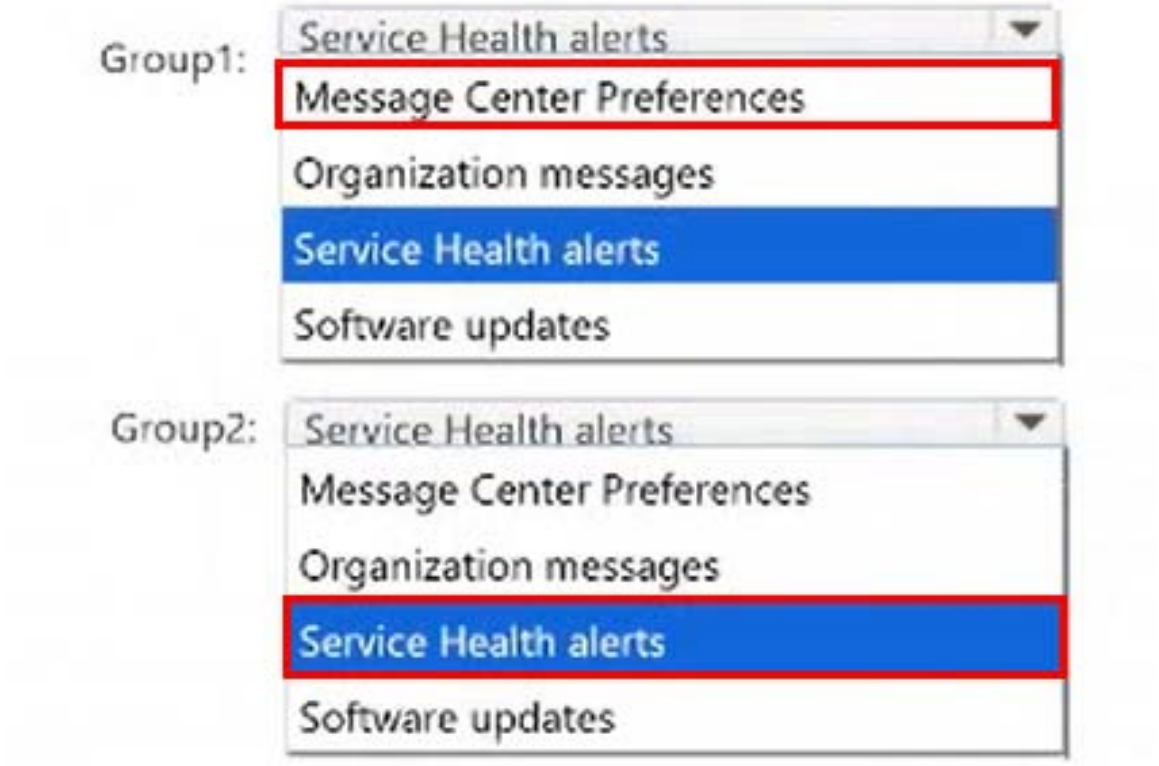
Group1: Receive email notifications when major service updates occur.

Group2: Receive email alerts when Microsoft 365 maintenance events occur.

Which type of notification should you configure for each group?



Answer:


Group1:
Service Health alerts
Message Center Preferences
Organization messages
Service Health alerts
Software updates
Group2:
Service Health alerts
Message Center Preferences
Organization messages
Service Health alerts
Software updates

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/