



Microsoft AB-650

Microsoft Administering Microsoft 365 and AI Services

Thank You for Downloading AB-650 Updated Exam Questions

<https://certs4sale.com/microsoft/ab-650-pdf-exam-dumps>

Version: 4.1

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:

Explanation:

Microsoft Entra administrative units support dynamic device membership based on device attributes. AU1 uses the following membership rule:

(device.deviceTrustType -eq "Workplace") -and

(device.deviceOSType -in ["Windows", "Android"])

Statement 1: No.

Admin1 holds the Global Administrator role. However, AU1 uses dynamic membership, which prevents administrators from manually adding or removing members. Membership is determined exclusively by the configured rule.

Additionally, Device1 is Microsoft Entra joined, corresponding to deviceTrustType = AzureAD, rather than Workplace. Therefore, Device1 does not satisfy the rule.

Statement 2: Yes.

Device2 runs Windows 11 and is Microsoft Entra registered.

Microsoft Entra registered devices have a deviceTrustType value of Workplace, and Windows matches the permitted operating system list. Therefore, Device2 satisfies both conditions and is automatically included in AU1.

Statement 3: Yes.

The planned Android devices must be Microsoft Entra registered. Registered Android devices satisfy the Workplace trust condition and, when their recorded operating system value is Android, also satisfy the OS condition.

Consequently, they are automatically added to AU1 through dynamic membership processing. Group1 membership itself does not determine AU1 membership.

Administrators should verify the actual deviceOSType value because some Android Enterprise registrations use more specific operating system identifiers.

Microsoft Reference:

Manage dynamic membership in administrative units.

Microsoft Entra dynamic membership rules and device attributes.

Question: 2

HOTSPOT

You need to implement CAPolicy1. The solution must meet the technical requirements.

Which two Conditional Access settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CAPolicy1 ✓

Assignments

Users or agents (Preview) ⓘ

[Specific users included](#)

Target resources ⓘ

[All resources \(formerly 'All cloud apps'\)](#)

Network ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant * ⓘ

0 controls selected

Session * ⓘ

0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ

User risk level is the likelihood that the user account is compromised.

Not configured

Sign-in risk ⓘ

Sign-in risk level is the likelihood that the sign-in session is compromised.

Not configured

Insider risk ⓘ

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Authentication flows ⓘ

Not configured

Answer:

Explanation:

Microsoft Entra Conditional Access integrates with Microsoft Entra ID Protection to evaluate risky authentication attempts and enforce additional security requirements based on detected sign-in risk.

The Contoso technical requirement states that Group3 users accessing Microsoft 365 resources from anonymous IP addresses must complete multifactor authentication (MFA).

First selection: Sign-in risk.

Microsoft Entra ID Protection recognizes sign-ins from anonymous IP addresses, including anonymous VPNs and Tor exit nodes, as potential security risks.

Administrators can configure the Sign-in risk condition in CAPolicy1 to evaluate authentication attempts based on their calculated risk level. Microsoft recommends considering medium and high sign-in risk for MFA enforcement, depending on the organization's security requirements.

Second selection: Grant.

The Grant access control determines which authentication requirements must be satisfied before access is permitted.

Administrators should select Grant access and configure the built-in Multifactor authentication strength, or the corresponding Require multifactor authentication control where available.

Because CAPolicy1 already targets Group3 and all resources, these selections apply risk-based MFA requirements to the intended users and Microsoft 365 resources.

Technical qualification: Sign-in risk policies operate on calculated risk levels, not exclusively on anonymous IP addresses. Consequently, they may also trigger for other risky sign-ins and cannot guarantee that every anonymous-IP connection is challenged.

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.

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

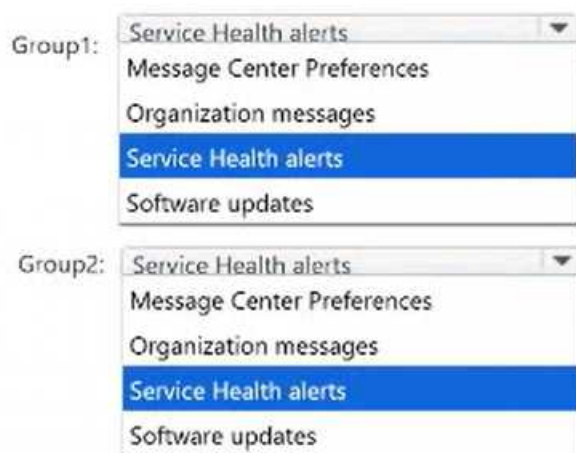
You have a Microsoft 365 subscription that contains two groups named Group1 and Group2.

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:

Explanation:

Microsoft 365 provides Message Center and Service Health notification mechanisms for communicating organizational service changes and operational issues.

First selection: Message Center Preferences. The Microsoft 365 Message Center publishes information about important product changes, feature releases, service updates, and administrative actions. Administrators can configure email preferences to receive notifications about major updates. This directly meets Group1's requirement.

Second selection: Service Health alerts. Service Health supports email notifications for incidents and advisories affecting Microsoft 365 services. Administrators can configure notifications for selected services and designate recipient email addresses. This is the likely intended selection for Group2 if maintenance events means operational service disruptions or advisories.

Microsoft documentation qualification: Planned maintenance is treated differently. Microsoft's

current documentation explicitly states that planned maintenance announcements appear in Message Center rather than the Service Health dashboard. Therefore, if Group2 requires notifications specifically about planned maintenance, Message Center is the appropriate source, and the proposed Service Health selection does not completely meet that requirement.

The distinction is important when implementing the configuration. Major product updates and planned maintenance communications belong to Message Center; active incidents and service advisories belong to Service Health.

Microsoft Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/message-center>

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

THANK YOU FOR DOWNLOADING AB-650 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our AB-650 Exam Product

Visit Our Site to Purchase the Full Set of Actual AB-650 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/microsoft/ab-650-pdf-exam-dumps>