AZ-500$^{\text{Q\&As}}$

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.passapply.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You plan to implement JIT VM access. Which virtual machines will be supported?

A. VM2, VM3, and VM4 only

B. VM1, VM2, VM3, and VM4

C. VM1 and VM3 only

D. VM1 only

Correct Answer: C

QUESTION 2

You have been tasked with delegate administrative access to your company\\'s Azure key vault.

You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.

Which of the following options should you use to achieve your goal?

A. A key vault access policy

B. Azure policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

QUESTION 3

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.

You need to identify which inventory assets are vulnerable to the most critical web app security risks.

Which Defender EASM dashboard should you use?

A. Attack Surface Summary

B. GDPRCompliance

C. Security Posture

D. OWASP Top 10

Correct Answer: D

Defender EASM provides four dashboards:

*

OWASP Top 10: this dashboard surfaces any assets that are vulnerable according to OWASP\\'s list of the most critical web application security risks. On this dashboard, organizations can quickly identify assets with broken access control,

cryptographic failures, injections, insecure designs, security misconfigurations and other critical risks as defined by OWASP. Incorrect:

*

Security Posture: this dashboard helps organizations understand the maturity and complexity of their security program based on the metadata derived from assets in your Approved inventory. It is comprised of technical and non-technical policies, processes and controls that mitigate risk of external threats. This dashboard provides insight on CVE exposure, domain administration and configuration, hosting and networking, open ports, and SSL certificate configuration.

*

Attack Surface Summary: this dashboard summarizes the key observations derived from your inventory. It provides a high-level overview of your Attack Surface and the asset types that comprise it, and surfaces potential vulnerabilities by severity (high, medium, low). This dashboard also provides key context on the infrastructure that comprises your Attack Surface, providing insight into cloud hosting, sensitive services, SSL certificate and domain expiry, and IP reputation.

*

GDPR Compliance: this dashboard surfaces key areas of compliance risk based on the General Data Protection Regulation (GDPR) requirements for online infrastructure that\\'s accessible to European nations. This dashboard provides insight on the status of your websites, SSL certificate issues, exposed personal identifiable information (PII), login protocols, and cookie compliance.

Note: Microsoft Defender External Attack Surface Management (Defender EASM) offers a series of four dashboards designed to help users quickly surface valuable insights derived from their Approved inventory. These dashboards help organizations prioritize the vulnerabilities, risks and compliance issues that pose the greatest threat to their Attack Surface, making it easy to quickly mitigate key issues.

Reference: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/understanding-dashboards

QUESTION 4

You need to meet the identity and access requirements for Group1.

What should you do?

A. Add a membership rule to Group1.

B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.

C. Modify the membership rule of Group1.

D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Correct Answer: D

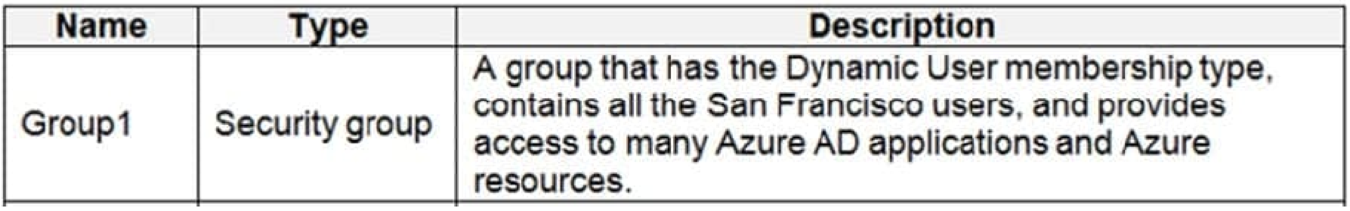
When you create dynamic groups, they can either contain users or devices. Hence here we need to create two separate dynamic groups and assign those groups to an Assigned group.

Incorrect Answers:

A, C: You can create a dynamic group for devices or users, but you can\\'t create a rule that contains both users and devices.

Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.



Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

The tenant currently contains this group:

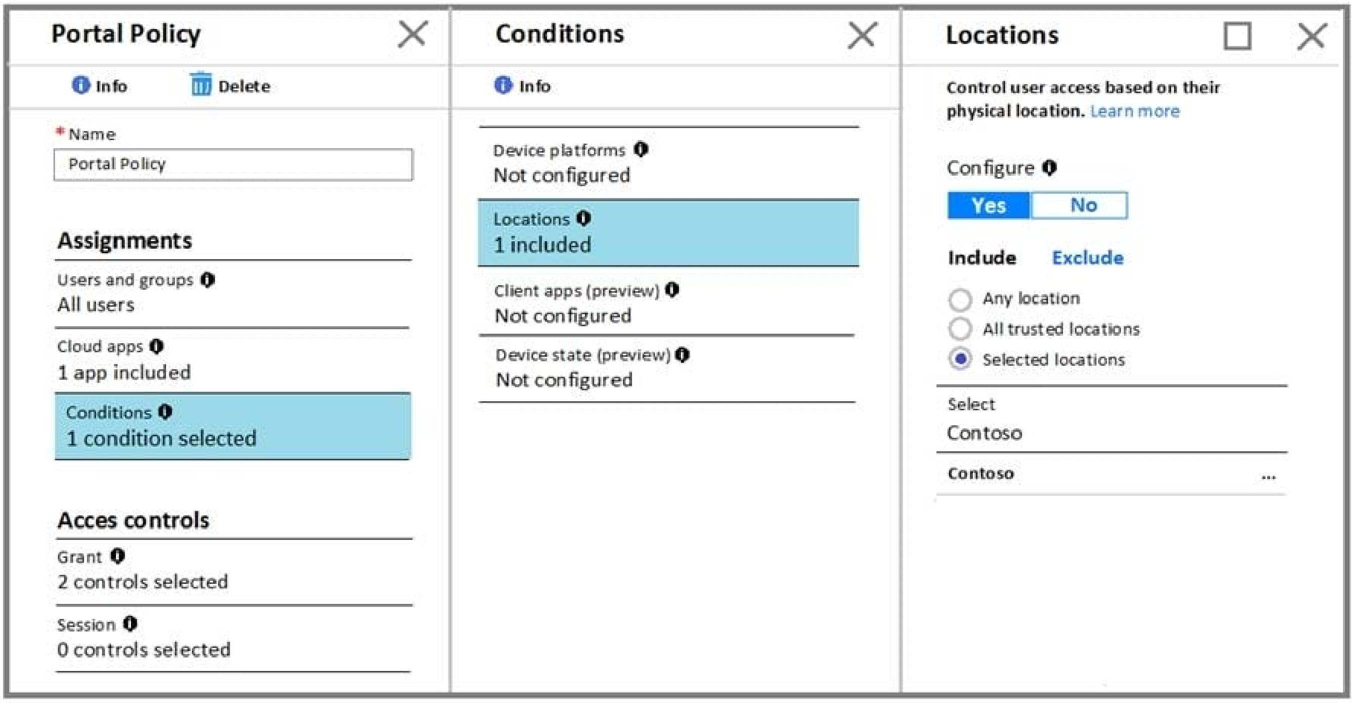
Reference: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

QUESTION 5

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



Portal Policy

Info | Delete

* Name: Portal Policy

Assignments

Users and groups: All users

Cloud apps: 1 app included

Conditions: 1 condition selected

Acces controls

Grant: 2 controls selected

Session: 0 controls selected

Conditions

Info

Device platforms: Not configured

Locations: 1 included

Client apps (preview): Not configured

Device state (preview): Not configured

Locations

Control user access based on their physical location. Learn more

Configure: [✓ Yes] No

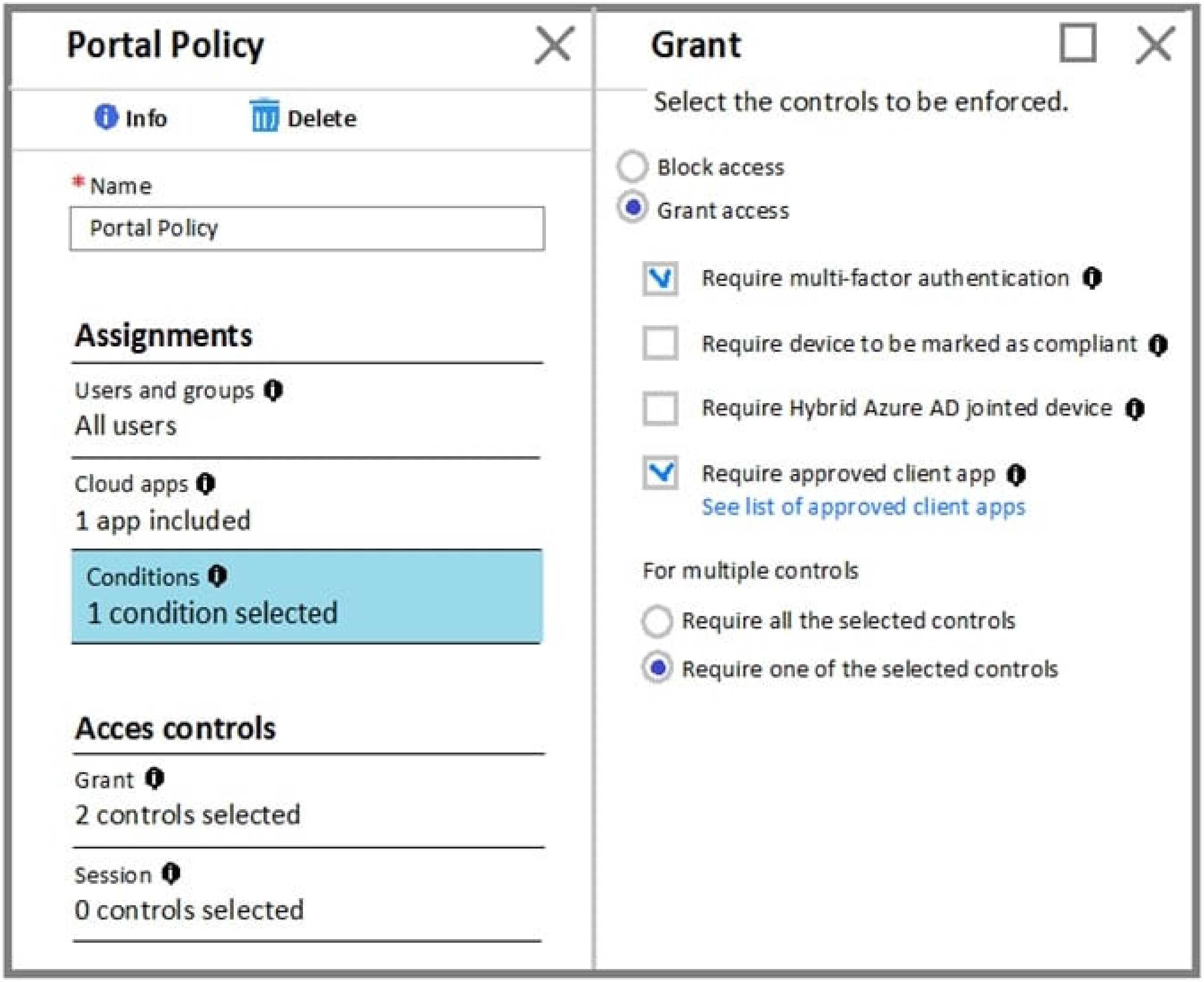
Include | Exclude

○ Any location
○ All trusted locations
● Selected locations

Select: Contoso

Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



Portal Policy

* Name
Portal Policy

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Acces controls

Grant
2 controls selected

Session
0 controls selected

Grant

Select the controls to be enforced.

○ Block access
● Grant access

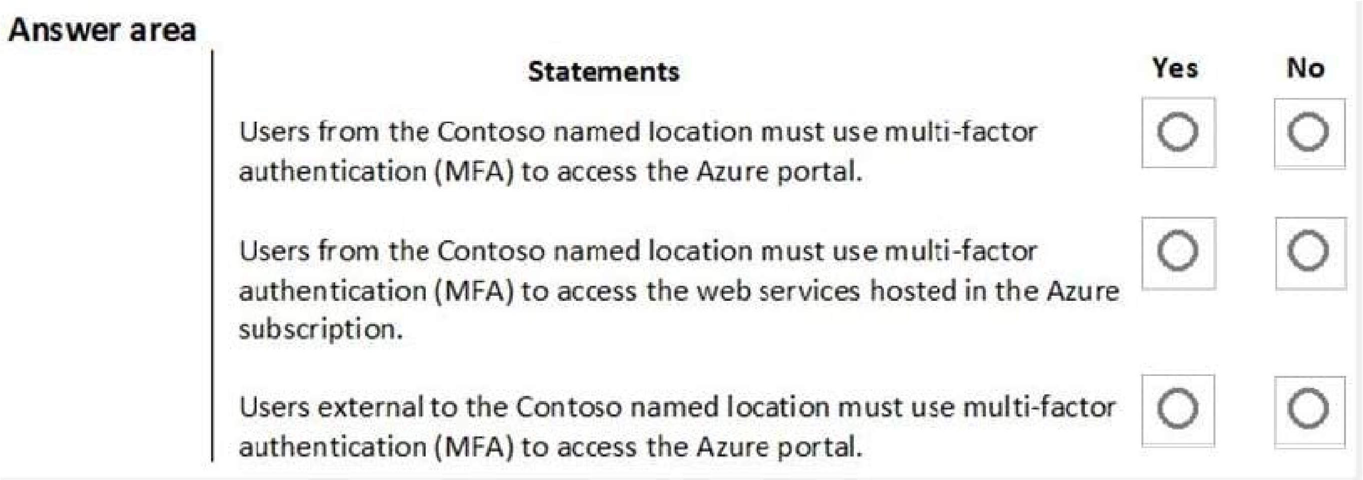
☑ Require multi-factor authentication
□ Require device to be marked as compliant
□ Require Hybrid Azure AD jointed device
☑ Require approved client app
See list of approved client apps

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

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

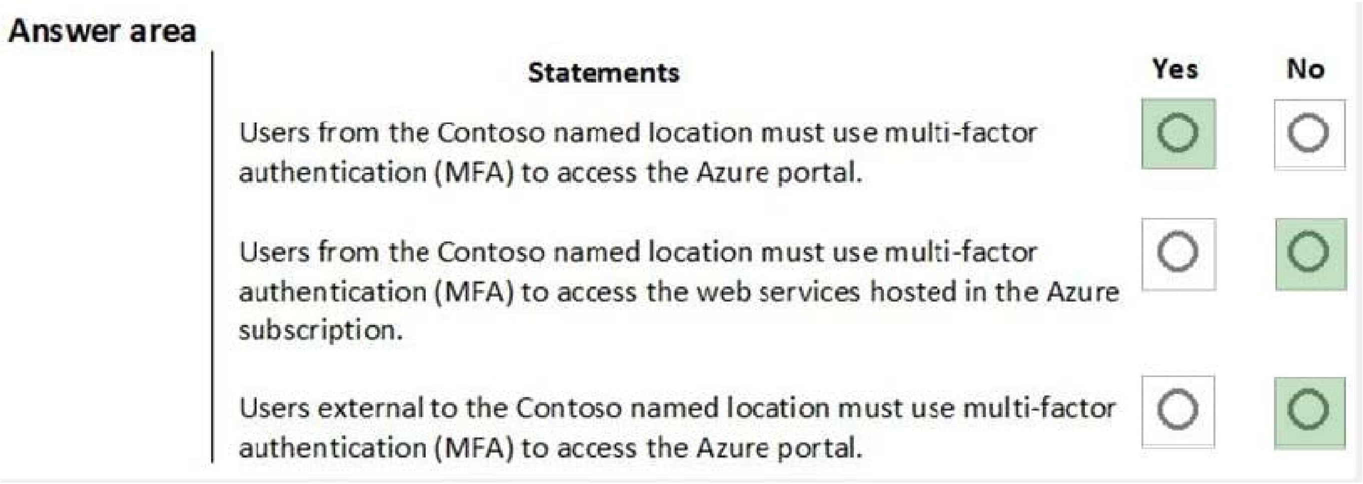
Hot Area:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

Correct Answer:



Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	[✓ ○]	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	[✓ ○]
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	[✓ ○]

YES - Contoso location requires MFA to use AZ Portal NO - Contoso location does not require MFA to use web NO - External users from Contoso location are not required to use MFA for AZ portal

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa?toc=/azure/active-directory/conditional-access/toc.jsonandbc=/azure/active-directory/conditional-access/breadcrumb/toc.json#configure-theconditions-for-multi-factor-authentication https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#microsoft-cloud-applications

[AZ-500 PDF Dumps] [AZ-500 Study Guide] [AZ-500 Exam Questions]