



SC-900^{Q&As}

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/sc-900.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



**QUESTION 1**

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. text message (SMS)
- B. Microsoft Authenticator app
- C. email verification
- D. phone call
- E. security question

Correct Answer: ABD

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

QUESTION 2**HOTSPOT**

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
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input checked="" type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input checked="" type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 3**HOTSPOT**

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
Software tokens are an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>
Windows Hello is an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>
FIDO2 security keys are an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication	<input type="radio"/>	<input checked="" type="radio"/>
Windows Hello is an example of passwordless authentication	<input checked="" type="radio"/>	<input type="radio"/>
FIDO2 security keys are an example of passwordless authentication	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No

Software tokens is a time-based one-time passcodes (TOTP) solution.

Microsoft Authenticator, which is a passwordless solution, uses software tokens though.

Note: Authentication methods in Azure Active Directory - OATH tokens

OATH TOTP (Time-based One Time Password) is an open standard that specifies how one-time password (OTP) codes are generated. OATH TOTP can be implemented using either software or hardware to generate the codes. Azure AD

doesn't support OATH HOTP, a different code generation standard.

OATH software tokens

Software OATH tokens are typically applications such as the Microsoft Authenticator app and other authenticator apps. Azure AD generates the secret key, or seed, that's input into the app and used to generate each OTP.

Box 2: Yes

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

Windows Hello for Business

Microsoft Authenticator

FIDO2 security keys

Box 3: Yes

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens>

**QUESTION 4****HOTSPOT**

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
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input checked="" type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input checked="" type="radio"/>

**QUESTION 5**

You need to ensure repeatability when creating new resources in an Azure subscription. What should you use?

- A. Microsoft Sentinel
- B. Azure Policy
- C. Azure Batch
- D. Azure Blueprints

Correct Answer: D

Using Azure Blueprints for repeatable deploy and update operations.

Sometimes, using policies is just not enough. Reasons may vary—the number of projects is too big to govern via policies, they become obstacles because you cannot enforce a particular rule, or you find complex designs with them to be just too complicated. For all of those scenarios, Microsoft has prepared an additional tool for Azure administrators called Azure Blueprints. They are like sketches for buildings—you can set collect all required artifacts in one place and use it for multiple deployments. With this feature, you can orchestrate multiple deployments and shorten the time needed to achieve a coherent architecture. If you are familiar with ARM templates, you may find Azure Blueprints much easier to understand as they offer similar functionalities to Resource Manager. On the other hand, it is a great tool for preserving a connection between a blueprint and a deployment or manage multiple subscriptions at once.

Reference: <https://subscription.packtpub.com/book/cloud-and-networking/9781838551452/2/ch02lv1sec13/using-azure-blueprints-for-repeatable-deploy-and-update-operations>

[SC-900 VCE Dumps](#)

[SC-900 Study Guide](#)

[SC-900 Braindumps](#)