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.leads4pass.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

What can you use to view the Microsoft Secure Score for Devices?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Endpoint

C. Microsoft Defender for Identity

D. Microsoft Defender for Office 365

Correct Answer: B

Artikel 3 Minuten Lesedauer Microsoft Secure Score for DevicesApplies to:

1.

Microsoft Defender for Endpoint Plan 2

2.

Microsoft Defender Vulnerability Management

3.

Microsoft 365 Defender

Some information relates to pre-released product which may be substantially modified before it\\'s commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com).

Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on.

Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat

attacks. It reflects the collective security configuration state of your devices across the following categories:

1.

Application

2.

Operating system

3.

Network

4.

Accounts

5.

Security controls

Select a category to go to the Security recommendations page and view the relevant recommendations.

Turn on the Microsoft Secure Score connectorForward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your

Microsoft Secure Score data.

Changes might take up to a few hours to reflect in the dashboard.

1.

In the navigation pane, go to Settings > Endpoints > General > Advanced features

2.

Scroll down to Microsoft Secure Score and toggle the setting to On.

3.

Select Save preferences.

How it worksMicrosoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured.

Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management.

The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:

1.

Compare collected configurations to the collected benchmarks to discover misconfigured assets

2.

Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction)

3.

Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams)

4.

Collect and monitor changes of security control configuration state from all assets

QUESTION 2

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

A. Microsoft Defender for Office 365

B. Microsoft Defender Antivirus

C. Microsoft Defender for Identity

D. Microsoft Defender for Endpoint

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

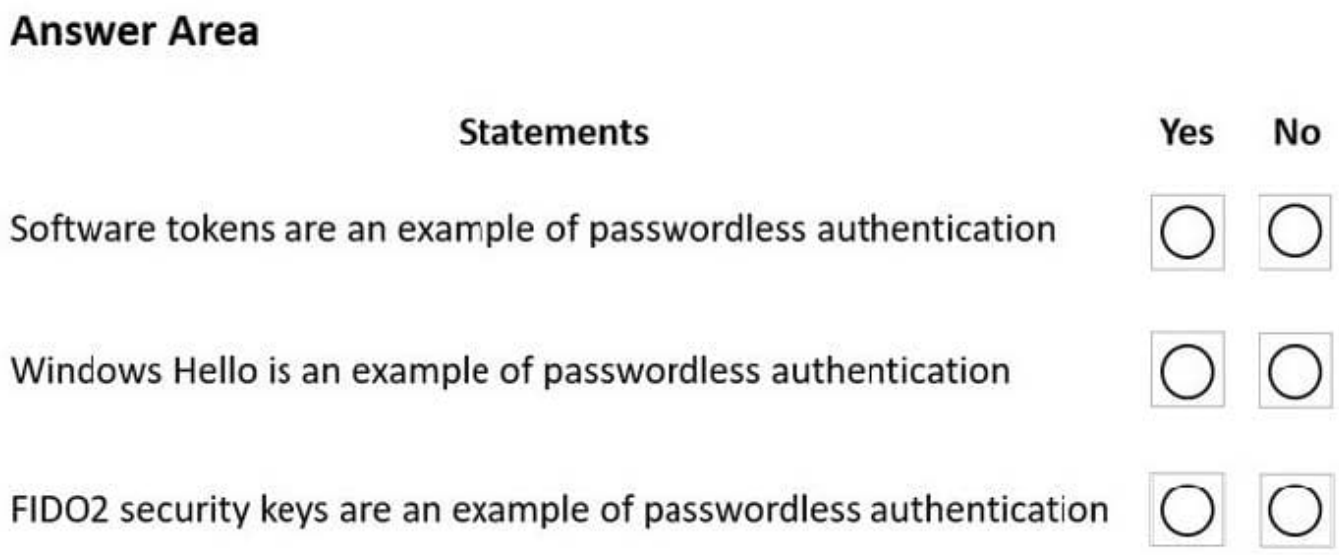
QUESTION 3

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:



Correct Answer:

Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication	○	◉
Windows Hello is an example of passwordless authentication	◉	○
FIDO2 security keys are an example of passwordless authentication	◉	○

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

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.

A user named User1 sends link-based, branded emails that are encrypted by using Microsoft Office 365 Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients can User1 revoke the emails?

A. Recipient4 only

B. Recipient1 only

C. Recipient1, Recipient2, Recipient3, and Recipient4

D. Recipient3 and Recipient4 only

E. Recipient1 and Recipient2 only

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

QUESTION 5

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
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Correct Answer:

Statements	Yes	No
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide