



**Free Questions for MS-102 by certsinside**

**Shared by Browning on 12-12-2023**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

## Question Type: MultipleChoice

---

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it As a result these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- \* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- \* User passwords must be 10 characters or more.

Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.

Does this meet the goal?

### Options:

---

A- Yes

B- No

### Answer:

---

B

## Question 2

---

### Question Type: MultipleChoice

---

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You purchase a Microsoft 365 subscription.

You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).

You need to ensure that users can use Seamless SSO from the Windows 10 computers.

What should you do?

### Options:

---

- A- Join the computers to Azure AD.
- B- Create a conditional access policy in Azure AD.
- C- Modify the Intranet zone settings by using Group Policy.
- D- Deploy an Azure AD Connect staging server.

### Answer:

---

A

## Question 3

---

### Question Type: MultipleChoice

---

Your network contains an Active Directory forest named Contoso. Local.

You have a Microsoft 365 subscription.

You plan to implement a directory synchronization solution that will use password hash synchronization.

From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.

You need to prepare the environment for the planned directory synchronization solution.

What should you do first?

**Options:**

---

- A-** From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
- B-** From the Microsoft 365 admin center verify the Contoso. Local domain name.
- C-** From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
- D-** From Active Directory Users and Computers, modify the UPN suffix for all users.

**Answer:**

---

A

## Question 4

---

**Question Type:** MultipleChoice

---

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- \* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- \* User passwords must be 10 characters or more.

Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

**Options:**

---

**A-** Yes

**B-** No

**Answer:**

---

A

## Question 5

---

**Question Type:** MultipleChoice

---

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Health agent was installed on all the servers.

You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**Options:**

---

- A- From Azure Cloud shell, run the Connect-Azure AD cmdlet.
- B- From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
- C- From Server1, change the Azure AD Connect Health Services Startup type to Automatic
- D- From Windows PowerShell, run the Register-AzureADConnectHealthsyncAgent cmdlet.
- E- From Server1, reinstall the Azure AD Connect Health agent

**Answer:**

---

D, E

## Question 6

---

**Question Type: MultipleChoice**

---

You have a Microsoft 365 subscription.

You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.

You need to change the email address used to verify the domain.

What should you do?



### Options:

---

- A- From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
- B- Add a TXT record to the DNS zone of the domain.
- C- From the domain registrar, modify the contact information of the domain.
- D- Modify the NS records for the domain.

### Answer:

---

C

## Question 7

---

### Question Type: MultipleChoice

---

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- \* Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- \* User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

**Options:**

---

**A-** Yes

**B-** No

**Answer:**

---

B

## Question 8

---

**Question Type: MultipleChoice**

---

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

Corporate policy states that user passwords must not include the word Contoso.

What should you do to implement the corporate policy?

**Options:**

---

- A-** From Azure AD Identity Protection, configure a sign-in risk policy.
- B-** From the Microsoft Entra admin center, create a conditional access policy.
- C-** From the Microsoft 365 admin center, configure the Password policy settings.
- D-** From the Microsoft Entra admin center, configure the Password protection settings.

**Answer:**

---

D

## Question 9

---

**Question Type: MultipleChoice**

---

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- \* Signs in to Microsoft Exchange Online from an anonymous IP address
- \* Signs in to Microsoft SharePoint Online from a device in New York City.
- \* Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

### Options:

---

- A- anonymous IP address only
- B- anonymous IP address and atypical travel
- C- anonymous IP address, atypical travel, and unfamiliar sign-in properties
- D- unfamiliar sign-in properties and atypical travel only
- E- anonymous IP address and unfamiliar sign-in properties only

### Answer:

---

A

## Question 10

---

**Question Type:** MultipleChoice

---

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

**Options:**

---

**A-** User2 and User4 only

**B-** User1 and User3 only

**C-** User1 only

**D-** User1, User2, User3, and User4

**Answer:**

---

C

**To Get Premium Files for MS-102 Visit**

**<https://www.p2pexams.com/products/ms-102>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/microsoft/pdf/ms-102>**

