MS-102$^{Q\&As}$

Microsoft 365 Certified: Enterprise Administrator Expert

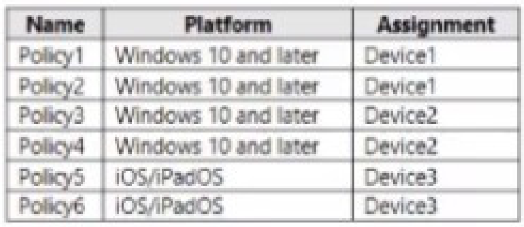
Pass Microsoft MS-102 Exam with 100% Guarantee

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

QUESTION 1

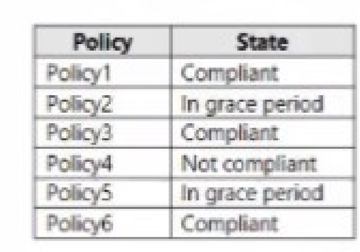
HOTSPOT

You have device compliance policies shown in the following table.



Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

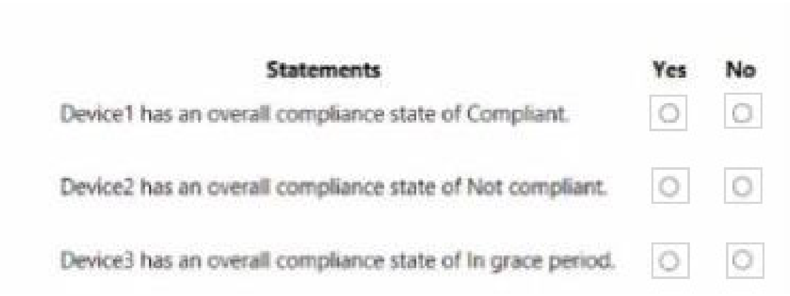
The device compliance state for each policy is shown in the following table.



Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

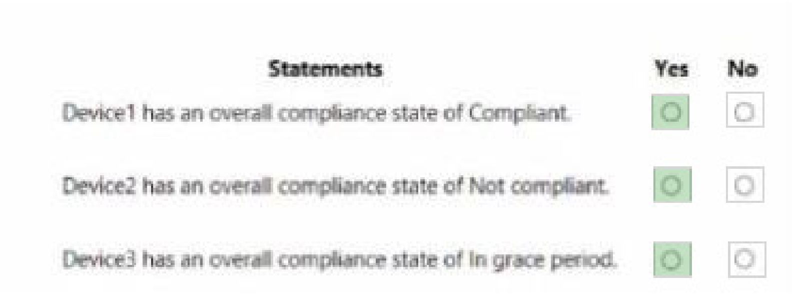
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

Correct Answer:

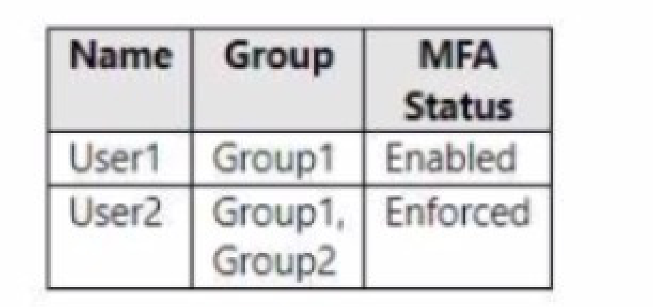


Statements	Yes	No
Device1 has an overall compliance state of Compliant.	[✓ ○]	○
Device2 has an overall compliance state of Not compliant.	[✓ ○]	○
Device3 has an overall compliance state of In grace period.	[✓ ○]	○

QUESTION 2

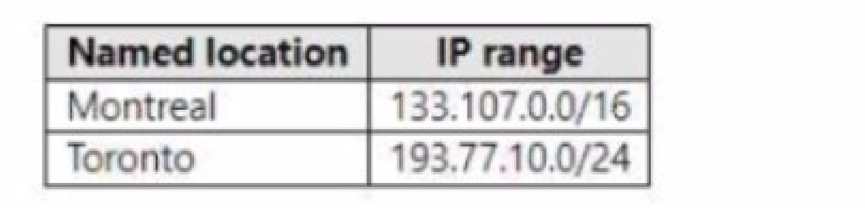
HOTSPOT

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



Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.



Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

Users or workload identities:

Include: Group1

Exclude: Group2

Cloud apps or actions: Include all cloud apps

Conditions:

Include: Any location

Exclude: Montreal

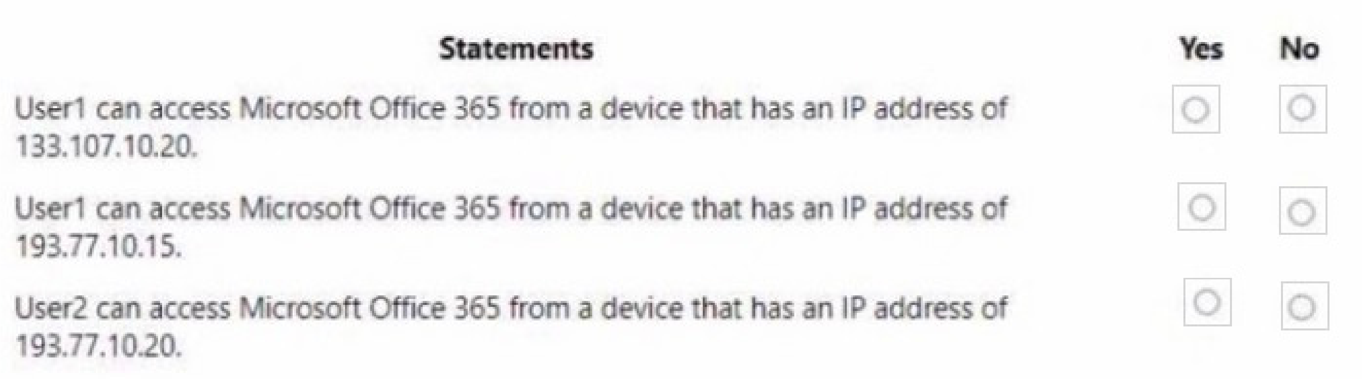
Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

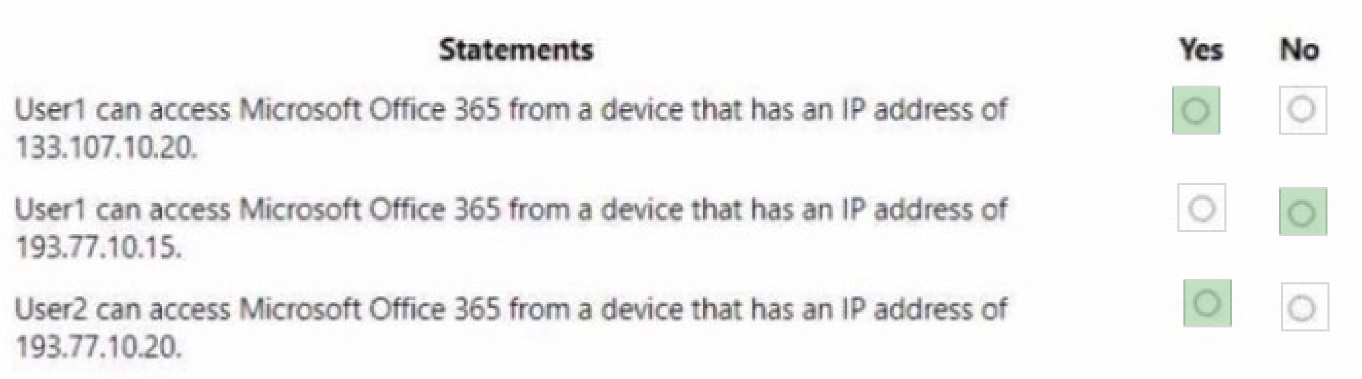
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	○	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	○
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	○	○

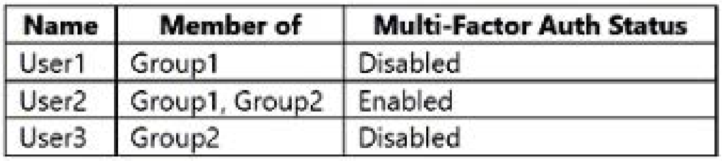
Correct Answer:



Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	[✓ ○]	○
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	○	[✓ ○]
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	[✓ ○]	○

QUESTION 3

HOTSPOT

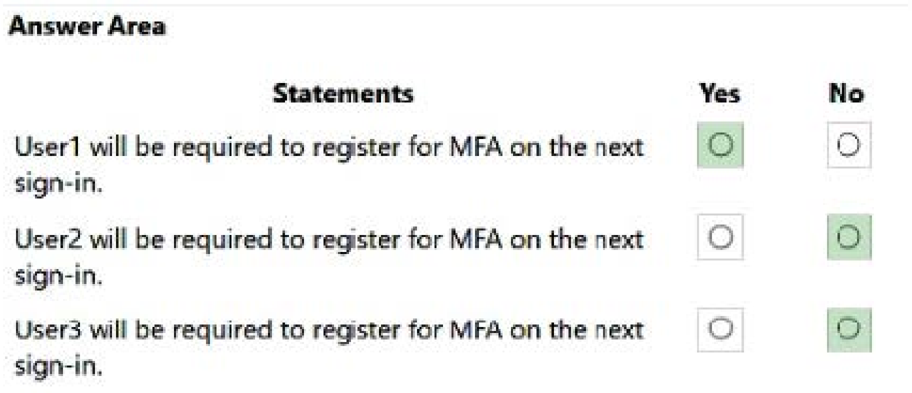


Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

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

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

Correct Answer:



Answer Area

Statements	Yes	No
User1 will be required to register for MFA on the next sign-in.	[✓ ○]	○
User2 will be required to register for MFA on the next sign-in.	○	[✓ ○]
User3 will be required to register for MFA on the next sign-in.	○	[✓ ○]

Statement 1 = Yes - User 1 is part of group 1 with MFA status disabled and, as per the MFA registration policy, will need to register for MFA.

Statement 2 = No - Although part of group one and two, they already have MFA enabled so will not need to register for it

Statement 3 = No - does not have MFA anebled already is part of group 2 so is excluded from registration policy, therefore will not need to register.

QUESTION 4

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to configure Microsoft Defender ATP on the computers.

What should you create from the Endpoint Management admin center?

A. a device configuration profile

B. an update policy for iOS

C. a Microsoft Defender ATP baseline profile

D. a mobile device management (MDM) security baseline profile

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

QUESTION 5

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.

User1 emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.

You need to prevent this issue from reoccurring.

What should you configure?

A. anti-spam policies

B. Safe Attachments policies

C. anti-phishing policies

D. anti-malware policies

Correct Answer: A

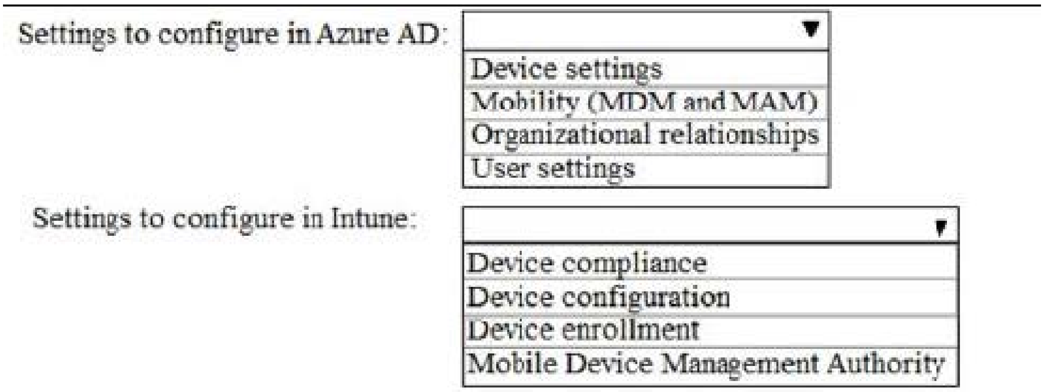
QUESTION 6

You need to meet the Intune requirements for the Windows 10 devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



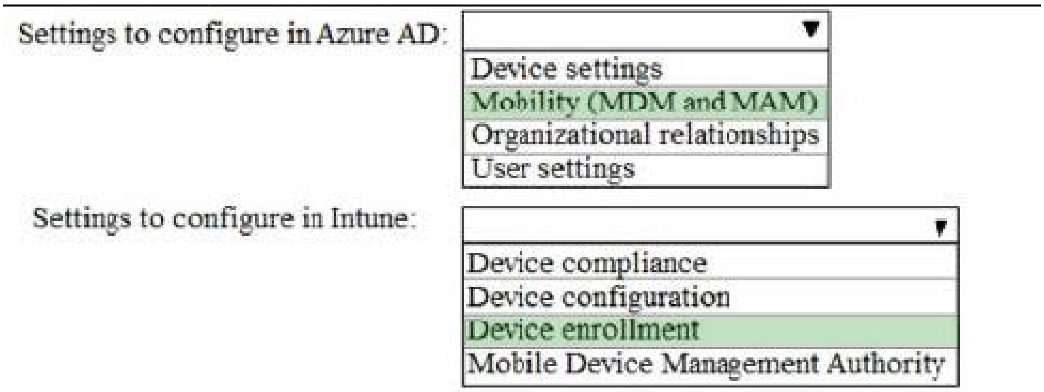
Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Correct Answer:



Settings to configure in Azure AD:

- Device settings
- [✓ Mobility (MDM and MAM)]
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- [✓ Device enrollment]
- Mobile Device Management Authority

References: https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION 7

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management.

Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only

B. Microsoft Teams only

C. Microsoft Exchanqe Online and SharePoint Online only

D. Microsoft Teams and SharePoint Online only

E. Microsoft Teams, Exchanqe Online, and SharePoint Online

Correct Answer: A

Privileged access management Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access- management-solution-overview

https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

QUESTION 8

HOTSPOT

You work at a company named Contoso, Ltd.

Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.

Contoso purchases a company named Fabrikam, Inc.

Contoso plans to add the following domains to the Microsoft 365 subscription:

fabrikam.com

east.fabrikam.com

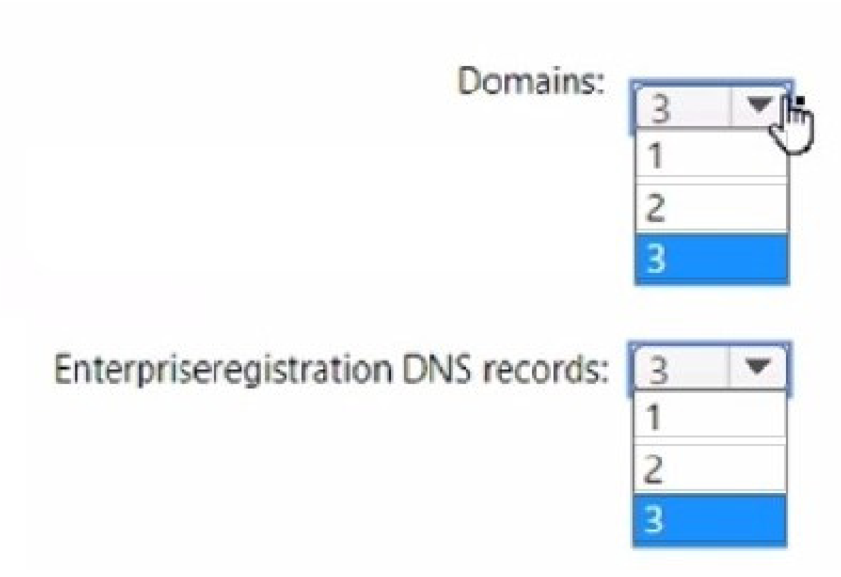
west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.

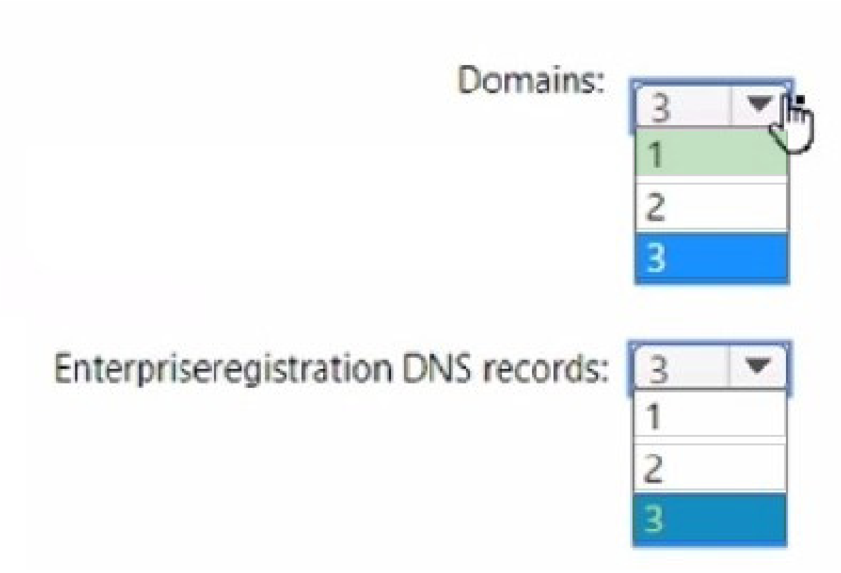
How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



1.

1 domain. Sub-domains don\\'t need to be verified, so just fabrikam.com.

2.

3 Enterpriseregistration DNS records. https://www.examtopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/

QUESTION 9

HOTSPOT

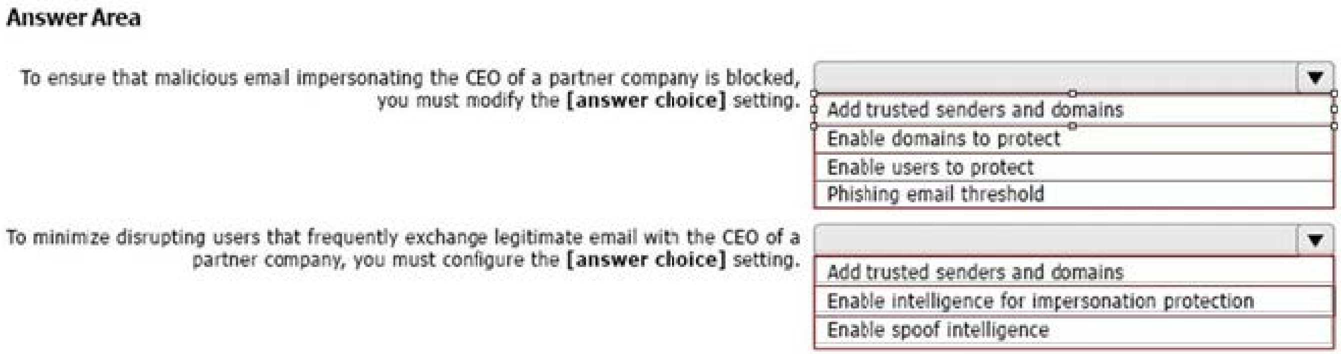
You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

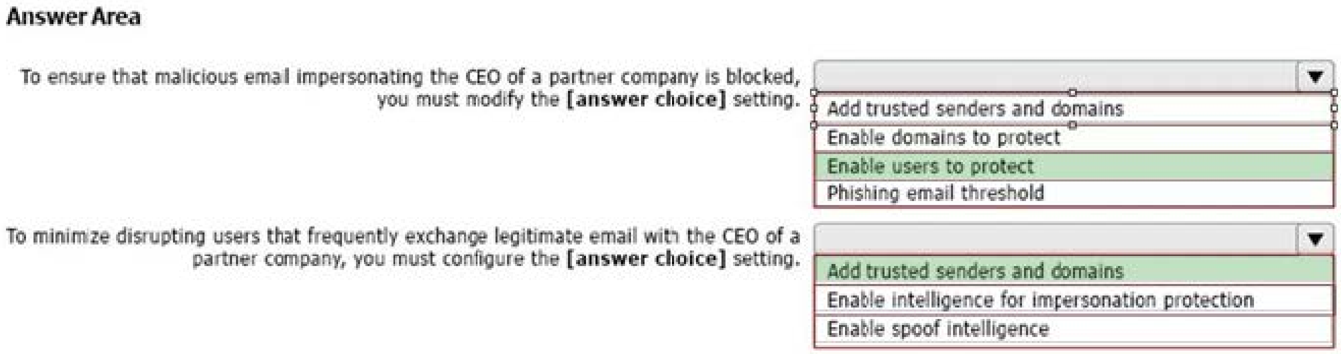
To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

Correct Answer:



Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.

- Add trusted senders and domains
- Enable domains to protect
- [✓ Enable users to protect]
- Phishing email threshold

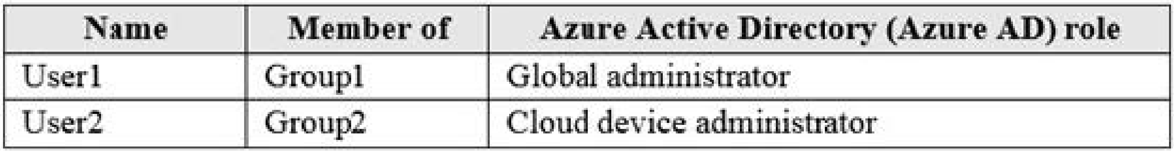
To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.

- [✓ Add trusted senders and domains]
- Enable intelligence for impersonation protection
- Enable spoof intelligence

QUESTION 10

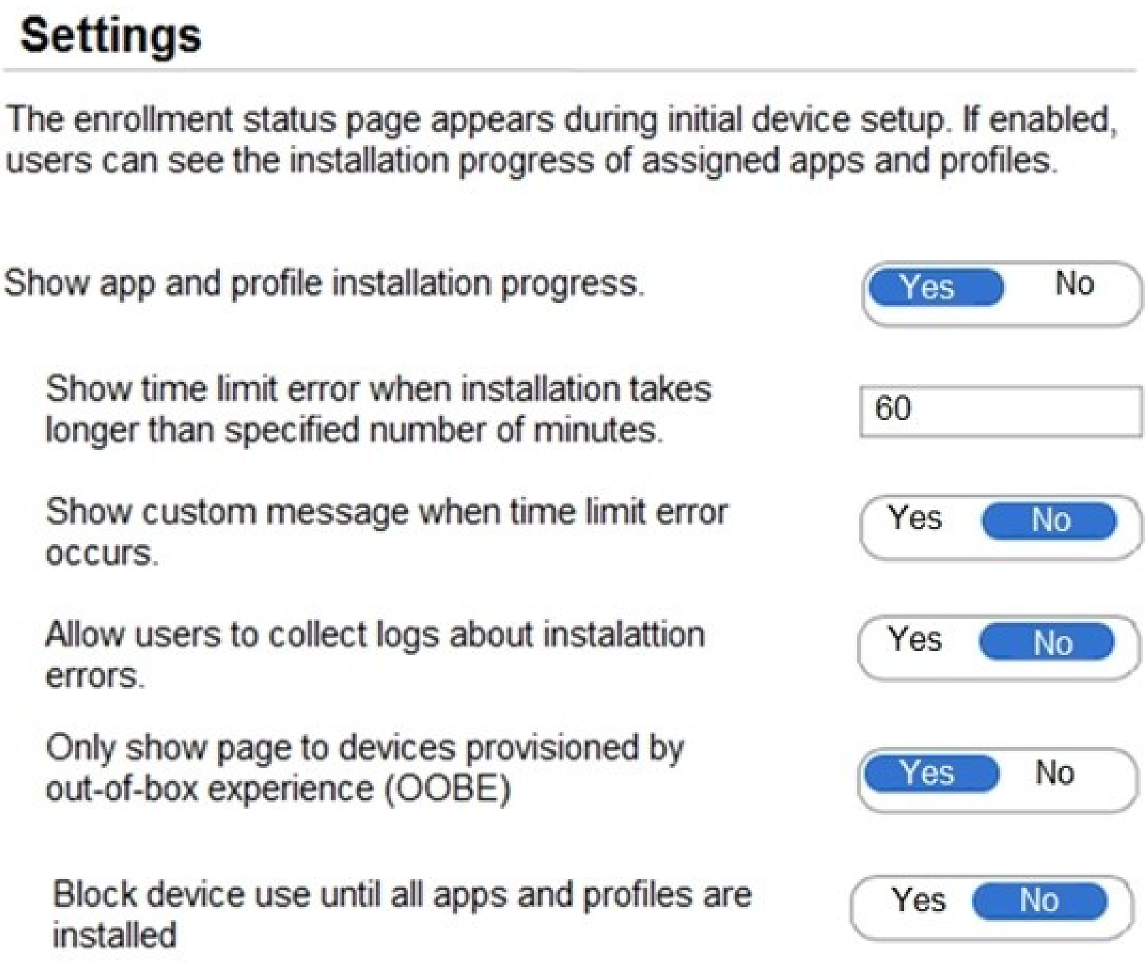
HOTSPOT

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



Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. [✓ Yes] No

Show time limit error when installation takes longer than specified number of minutes. 60

Show custom message when time limit error occurs. Yes [✓ No]

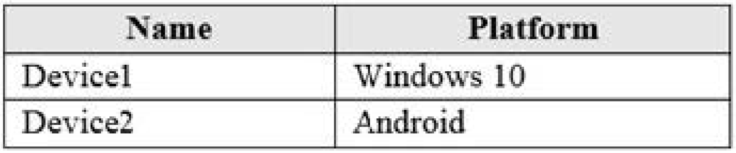
Allow users to collect logs about instalattion errors. Yes [✓ No]

Only show page to devices provisioned by out-of-box experience (OOBE) [✓ Yes] No

Block device use until all apps and profiles are installed Yes [✓ No]

You assign the policy to Group1.

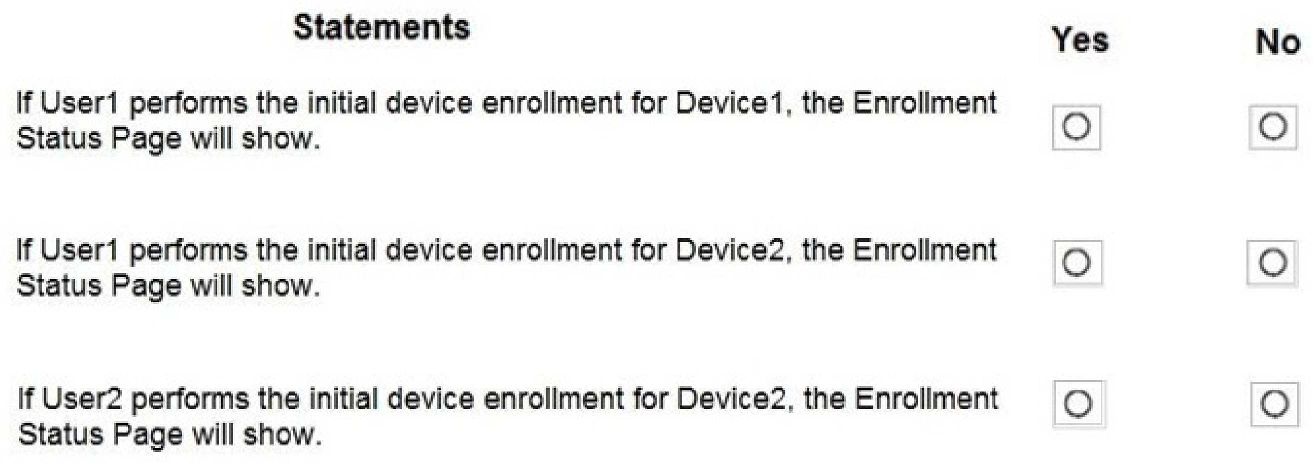
You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

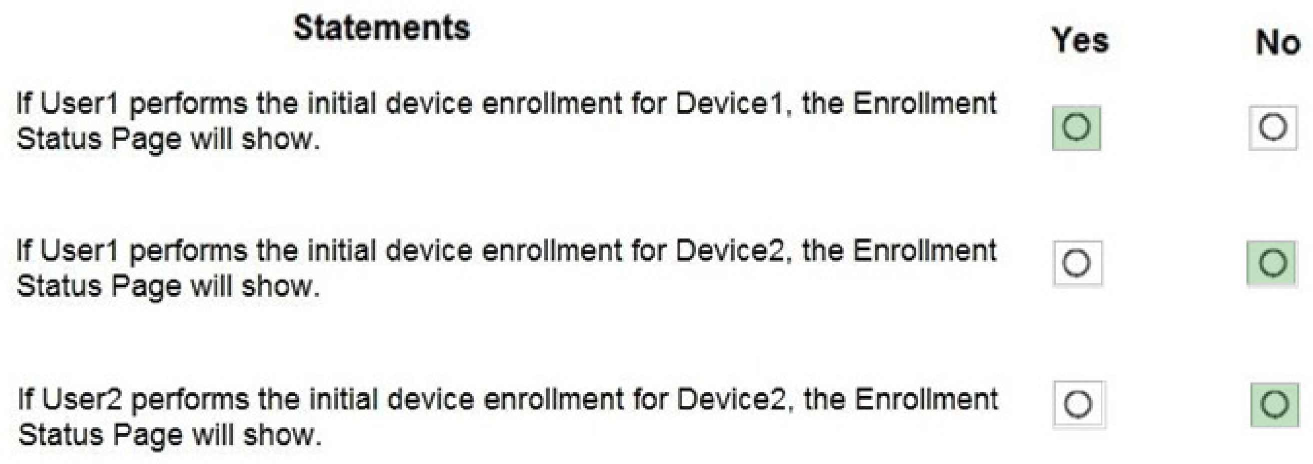
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

Correct Answer:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	[✓ ○]	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]

QUESTION 11

HOTSPOT

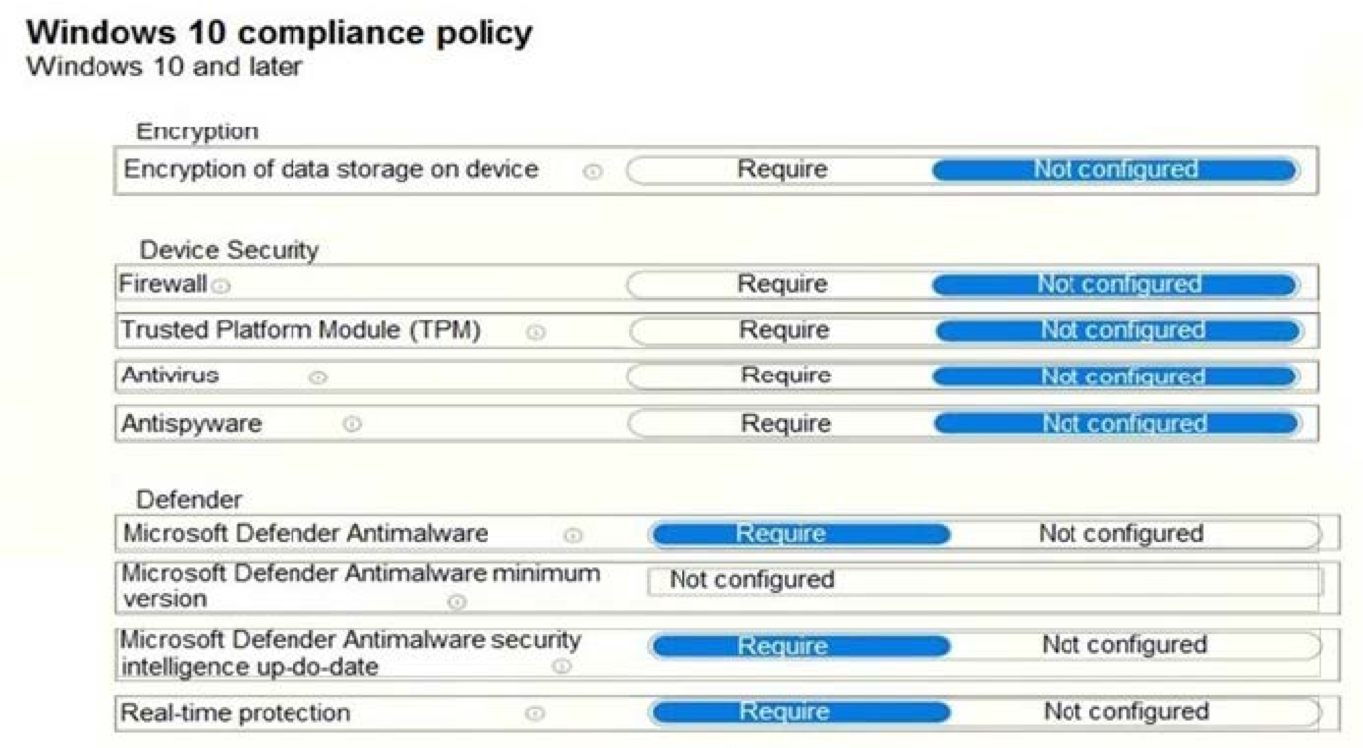
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices. You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device	Require [✓ Not configured]

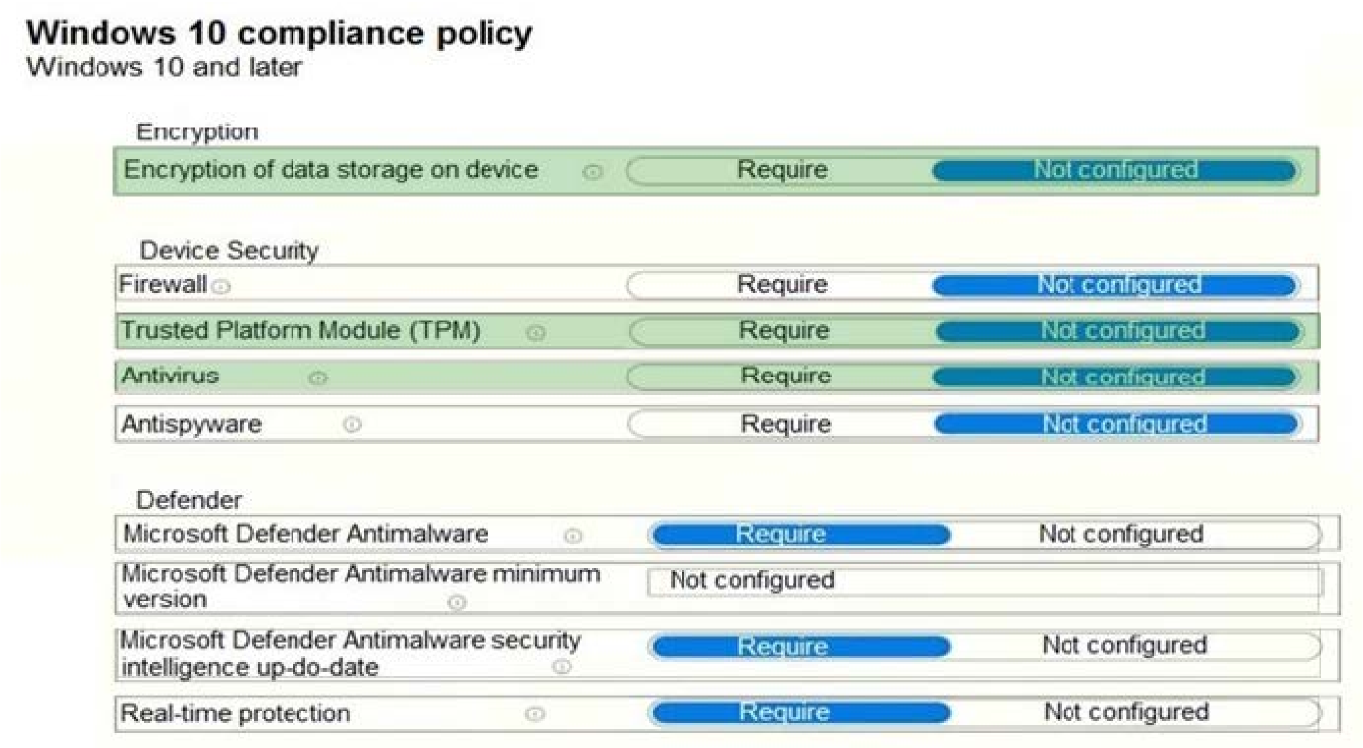
Device Security

Firewall	Require [✓ Not configured]
Trusted Platform Module (TPM)	Require [✓ Not configured]
Antivirus	Require [✓ Not configured]
Antispyware	Require [✓ Not configured]

Defender

Microsoft Defender Antimalware	[✓ Require] Not configured
Microsoft Defender Antimalware minimum version	Not configured
Microsoft Defender Antimalware security intelligence up-do-date	[✓ Require] Not configured
Real-time protection	[✓ Require] Not configured

Correct Answer:



Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device	Require [✓ Not configured]

Device Security

Firewall	Require [✓ Not configured]
Trusted Platform Module (TPM)	Require [✓ Not configured]
Antivirus	Require [✓ Not configured]
Antispyware	Require [✓ Not configured]

Defender

Microsoft Defender Antimalware	[✓ Require] Not configured
Microsoft Defender Antimalware minimum version	Not configured
Microsoft Defender Antimalware security intelligence up-do-date	[✓ Require] Not configured
Real-time protection	[✓ Require] Not configured

QUESTION 12

You have a Microsoft 365 E5 tenant, industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey

B. From Compliance Manager, create an assessment

C. From the Microsoft J6i compliance center, create an audit retention policy.

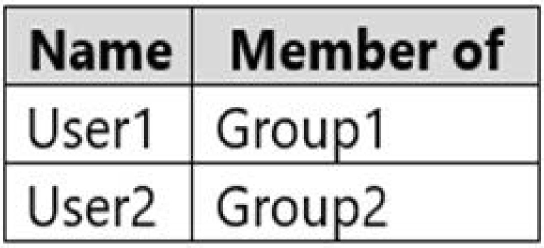
D. From the Microsoft 365 admin center enable the Productivity Score.

Correct Answer: B

QUESTION 13

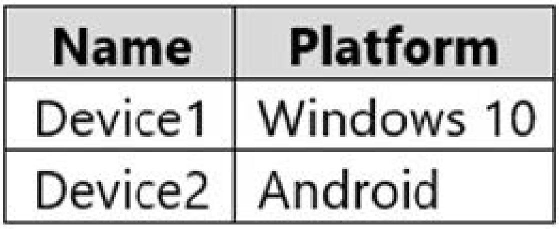
HOTSPOT

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



Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

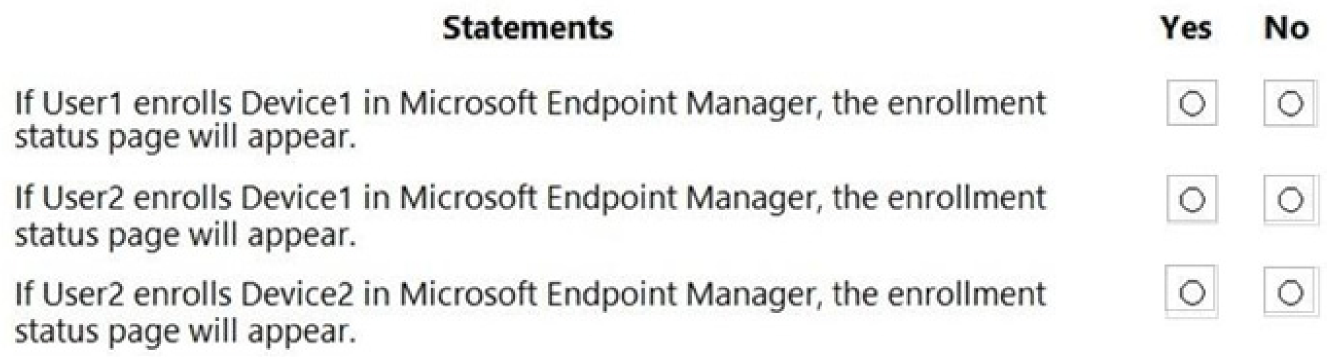
Show app and profile configuration progress: Yes

Allow users to collect logs about installation errors: Yes Only show page to devices provisioned by out-of-box experience (OOBE): No Assignments: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

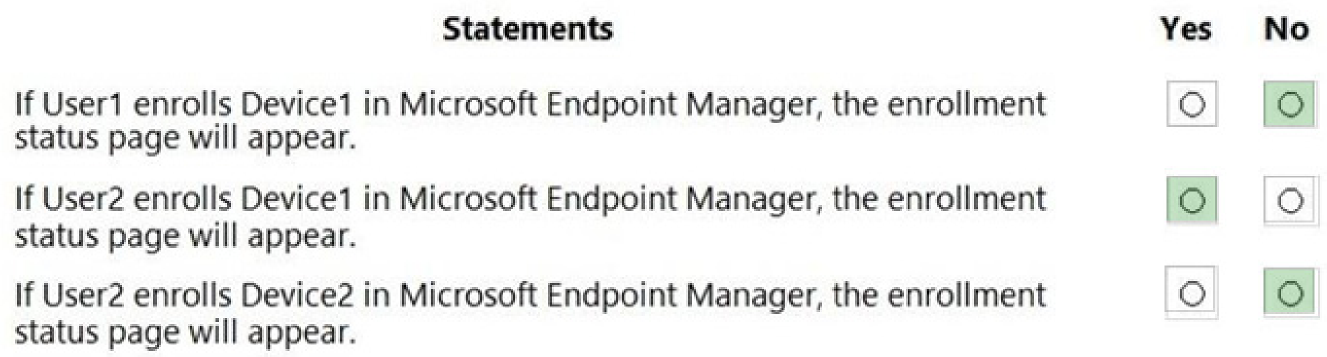
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

Correct Answer:



Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[✓ ○]
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	[✓ ○]	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[✓ ○]

QUESTION 14

Your company has a Microsoft Entra tenant named contoso.com and a Microsoft 365 subscription.

All users use Windows 10 devices to access Microsoft Office 365 apps.

All the devices are in a workgroup.

You plan to implement password less sign-in to contoso.com.

You need to recommend changes to the infrastructure for the planned implementation.

What should you include in the recommendation?

A. Join all the devices to contoso.com.

B. Deploy Microsoft Entra Application Proxy.

C. Deploy X.509.3 certificates to all the users.

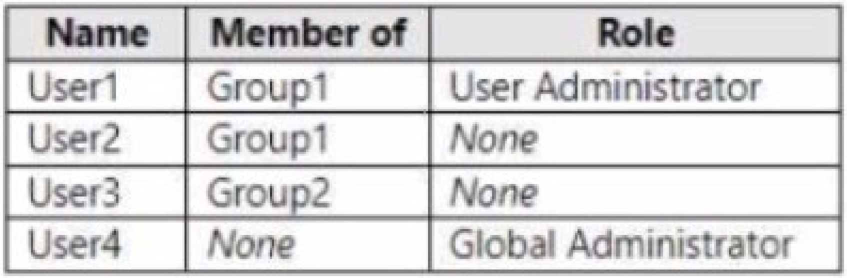
D. Deploy the Microsoft Authenticator app.

Correct Answer: D

QUESTION 15

HOTSPOT

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

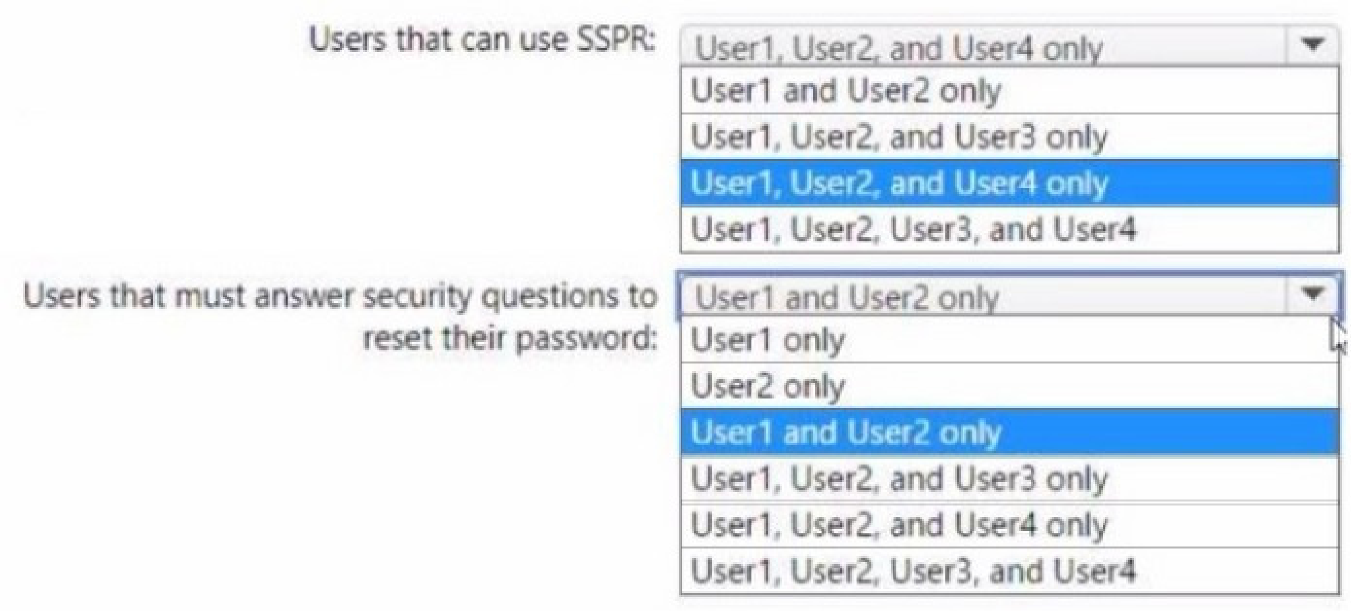


Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	*None*
User3	Group2	*None*
User4	*None*	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR. Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



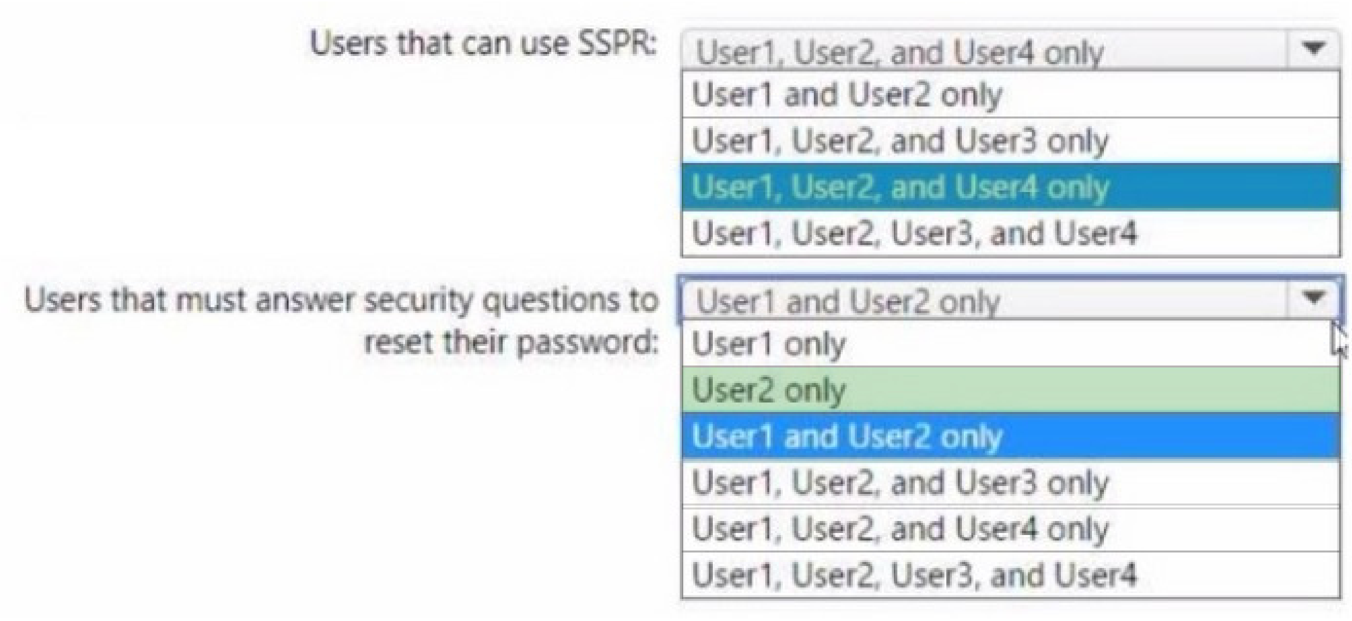
Users that can use SSPR: User1, User2, and User4 only

- User1 and User2 only
- User1, User2, and User3 only
- [✓ User1, User2, and User4 only]
- User1, User2, User3, and User4

Users that must answer security questions to reset their password: User1 and User2 only

- User1 only
- User2 only
- [✓ User1 and User2 only]
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Correct Answer:



Users that can use SSPR: User1, User2, and User4 only

- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Users that must answer security questions to reset their password: User1 and User2 only

- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Latest MS-102 Dumps MS-102 VCE Dumps MS-102 Study Guide