

Question: 108**HOTSPOT**

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

Name	Department
User1	Marketing
User2	Marketing
User3	Engineering
User4	Engineering
User5	Finance
User6	Finance

The tenant contains the administrative units shown in the following table.

Name	Description
AU1	Contains all the users in the marketing department Contains all the resources for the marketing department Contains User1 and User2
AU2	Contains all the users in the engineering department Contains all the resources for the engineering department Contains User3 and User4
AU3	Contains Group4, User5, and User6,

The tenant contains the groups shown in the following table.

Name	Administrative unit	Members
Group1	AU1	User1, User2
Group2	AU2	User3, User4
Group3	AU3	User5, User6
Group4	AU3	User1, User2, User3, User4, User5, User6

You perform the following actions:

- Assign User1 the User Administrator role for AU2.
- Assign User3 the Groups Administrator role for AU1.
- Assign User5 the Authentication Administrator role for AU3.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	☐	☐
User3 can add User4 to Group2.	☐	☐
User5 can configure an authentication method policy that requires all Group4 members to use passwordless sign-in.	☐	☐

Question: 110**HOTSPOT**

-

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

Name	Role
Admin1	Global Administrator
Admin2	Attribute Assignment Administrator
User1	User

The tenant contains the identities shown in the following table.

Name	Type
Group1	Security group
Service1	Service principal

You have an attribute set named Custom1 that contains the custom security attributes shown in the following table.

Name	Type
Attribute1	String
Attribute2	Integer

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

NOTE: Each correct selection is worth one point.

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

Answer Area

Statements	Yes	No
Admin1 can assign Attribute1 to User1.	☐	☐
Admin2 can modify Attribute1.	☐	☐
Admin2 can assign Attribute2 to Goup1.	☐	☐

Question: 111**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains two administrative units named AU1 and AU2. You create five users as shown in the following table.

Name	Administrative unit	Role	Role scope
User1	AU2	Global Administrator	None
User2	AU2	Helpdesk Administrator	AU1
User3	AU1	Privileged Authentication Administrator	AU2
User4	AU1	Helpdesk Administrator	AU1
User5	AU1	None	None

For which users can User2 and User3 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User2 can reset password for:

▼

User1 and User4 only
User1, User3, User4, and User5
User3 only
User4 only
User5 only

User3 can reset password for:

▼

User1 only
User1 and User2 only
User1, User2, and User4
User2 and User4 only
User 5 only

Question: 112**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 needs to perform the following tasks:

- Create a Microsoft 365 group named Group1 that has dynamic user membership
- Assign a Microsoft Entra Suite license to Group1.

In which portals can User1 perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create Group1:

- Microsoft Entra admin center only
- Microsoft 365 admin center only
- Microsoft Entra admin center and Microsoft 365 admin center only
- Microsoft Entra admin center and Microsoft Intune admin center only
- Microsoft Entra admin center, Microsoft 365 admin center, and Microsoft Intune admin center

Assign a Microsoft Entra Suite license to Group1:

- Microsoft Entra admin center only
- Microsoft 365 admin center only
- Microsoft Entra admin center and Microsoft 365 admin center only
- Microsoft Entra admin center and Microsoft Intune admin center only
- Microsoft Entra admin center, Microsoft 365 admin center, and Microsoft Intune admin center

Question: 113**HOTSPOT**

You have a Microsoft Entra tenant named contoso.com that contains a group named Group1. Group1 contains 50 users in your company's IT department and 50 users in your company's accounts department.

You have a partner company that has a Microsoft Entra tenant named fabrikam.com.

You configure cross-tenant synchronization between contoso.com and fabrikam.com.

You need to sync the members of Group1 to fabrikam.com. The solution must meet the following requirements:

- Ensure that only the IT department users sync with fabrikam.com.
- Minimize administrative effort.

What should you do in the Cross-tenant synchronization settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

For the configuration object:

▼

From Expression builder, build an expression.

From Provision on demand, add Group1.

From Users and groups, add Group1.

From Users and groups, add the IT department users

For the configuration object from Settings:

▼

Add a scoping filter

Add new attribute mappings

Modify the attribute mappings

Question: 114**HOTSPOT**

You have a Microsoft 365 tenant that contains the administrative units shown in the following table.

Name	Membership type	Restricted management	Dynamic membership rule
AU1	Dynamic user	Disabled	(user.department –eq “Department1”)
AU2	Dynamic user	Disabled	(user.department –eq “Department2”)

The subscription contains the administrators shown in the following table.

Name	Role	Role assignment scope
Admin1	Password Administrator	AU1
Admin2	Password Administrator	AU2
Admin3	Password Administrator	Global

The subscription contains the users shown in the following table.

Name	Department
User1	Department1
User2	Department1
User3	Department2

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin2 can reset the password of User2.	☐	☐
Admin3 can reset the password of User3.	☐	☐

Question: 126

DRAG DROP -

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions**Answer Area**

From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.



Question: 128

CertyIQ

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.

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Question: 129

CertyIQ

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.

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Question: 130

CertyIQ

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.

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Question: 131

HOTSPOT -

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements:

- ⇒ Identify sign-ins by users who are suspected of having leaked credentials.
- ⇒ Flag the sign-ins as a high-risk event.
- ⇒ Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection
Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Identity Governance
Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication
Device state
Sign-in risk
User location
User risk

To mitigate the risk, select:

Apply app enforced restrictions
Block access
Grant access but require app protection policy
Grant access but require password change