

Question: 428

CertyIQ

HOTSPOT

-

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the identities shown in the following table.

Name	Type	Role
------	------	------

in the following table.

Name	Type	Role
User1	User	Helpdesk Administrator
User2	User	Conditional Access Administrator
Group1	Group	Global Administrator
Group2	Group	Exchange Administrator
App1	Registered app	Authentication Administrator

The tenant is onboarded to Permissions Management.

You create the Azure resources shown in the following table.

Name	Type	Role
Managed1	Managed identity	Owner
Managed2	Managed identity	Cloud Application Administrator
SPrincipal1	Service principal	Security Operator

From Microsoft Entra Insights, which identity will be included in Accounts assigned to highly privileged roles, and which identity will be included in Service principals with privileged role assignments?

Answer Area

Accounts assigned to highly privileged roles:

User1
User2
Group1
Group2

Service principals with privileged role assignments:

App1
Managed1
Managed2
SPrincipal1

Question: 433

HOTSPOT

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

Name	Type
User1	Member
User2	Guest
User3	Member

The tenant contains the Microsoft 365 groups shown in the following table.

Name	Membership type	Role assignment allowed	Members
Group1	Assigned	Yes	User1, User2
Group2	Assigned	No	User1, User3
Group3	Dynamic user	No	User2, User3

You create an access review named Access1 that has the following settings:

- Select what to review: Teams + Groups
- Review scope: All Microsoft groups with guest users
- Scope: Guest users only
- Select reviewers: Users review their own access

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 review their membership in Group1 by using Access 1.	☐	☐
User2 can review their membership in Group3 by using Access1.	☐	☐
User3 can review their membership in Group2 by using Access1.	☐	☐

Question: 434**HOTSPOT**

-

You have an Azure subscription that contains a group named Group1 and two users named User1 and User2. User1 is a member of Group1.

You register an enterprise application named App1.

You enable self-service application access for App1 and configure the following settings:

- Allow users to request access to this application: Yes
- To which group should assigned users be added: Group1
- Require approval before granting access to this application: Yes
- Who is allowed to approve access to this application: User2

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 must request access to App1 before they can use the app.

☐☐

If User2 requests access to App1, they will be added to Group1 automatically.

☐☐

User2 can approve App1 requests by using the Microsoft Entra admin center.

☐☐

Question: 437

CertyIQ

HOTSPOT

You have a Microsoft Entra ID P2 tenant that contains four users named User1, User2, User3, and User4. The tenant contains the groups shown in the following table.

Name	Owner	Members
Group1	User2	User1, User3, User4
Group2	User2	User2

Group2 is onboarded to Privileged Identity Management (PIM).

You assign Group2 the roles shown in the following table.

Member	Role	Assignment type
User1	Member	Eligible
Group1	Member	Eligible
User4	Owner	Active

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
User2 can request to become a member of Group1 by using PIM.	☐	☐
User3 can request to become a member of Group2 by using PIM.	☐	☐
User4 can request to become a member of Group2 by using PIM.	☐	☐

Answer:

Statement 1: YesStatement 2: NoStatement 3: Yes

Question: 458

CertyIQ

Introductory Info Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

Question HOTSPOT -

You need to implement the planned changes and technical requirements for the marketing department. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure user access:

	▼
An access package	
An access review	
A conditional access policy	

To enable collaboration with fabrikam.com:

	▼
An accepted domain	
A connected organization	
A custom domain name	

Question: 459

Introductory Info Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question You need to meet the planned changes for the User administrator role.

What should you do?

- A. Create an access review.
- B. Create an administrative unit.
- C. Modify Active assignments.
- D. Modify Role settings.

Question: 460

CertyIQ

Introductory Info Case Study -
Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain

contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers. The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to modify the settings of the User administrator role to meet the technical requirements.
Which two actions should you perform for the role? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation.
- B. Select Require ticket information on activation.
- C. Modify the Expire eligible assignments after setting.
- D. Set all assignments to Eligible.
- E. Set all assignments to Active.

Question: 461

CertyIQ

Introductory Info Case Study -
Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.