

Question: 355

CertyIQ

HOTSPOT -

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

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 allow access for users who have fabrikam.com email addresses, configure:

☐	An access package assignment in Identity Governance
☐	An access package policy in Identity Governance
☐	A conditional access policy in Azure AD
☐	The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

☐	An access package assignment in Identity Governance
☐	An access package policy in Identity Governance
☐	A conditional access policy in Azure AD
☐	The External collaboration settings in Azure AD

Question: 370

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3.

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles



Edit

Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(s)

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)

Require Azure Multi-Factor Authentication on acti...	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the Application administrator role.
You configure User2 to be eligible for the Application administrator role.
For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)

Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

Assignment type ⓘ

☒ Eligible

☐ Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts *

01/01/2021



12:00:00 AM

Assignment ends *

01/31/2021



11:59:00 PM

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 is assigned the Application administrator role automatically.	☐	☐
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	☐	☐
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	☐	☐

Question: 427

CertyIQ

HOTSPOT

You have an Azure subscription that is onboarded to Microsoft Entra Permissions Management. You need to perform the following actions:

- Identify billable Azure resources.
- Create a rule to remove permissions for unused resources.

Which two options should you use in the Entra Permissions Management portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

