

Question: 244**HOTSPOT**

-

You have a Microsoft 365 E5 subscription that contains three groups named Group1, Group2, and Group3, and the users shown in the following table.

Name	Role	Member of
User1	Global Administrator	Group1
User2	None	Group2
User3	Global Reader	Group2, Group3

You create a Conditional Access policy named CA1 that has the following settings:

•Users

o Include

- Users and groups: Group1

o Exclude

- Users and groups: Group2

- Directory roles: Global Administrator

o Target resources

- Include: All cloud apps

o Access controls

- Grant: Require multifactor authentication

You create a Conditional Access policy named CA2 that has the following settings:

•Users

o Include

- Users and groups: Group2

o Exclude

- Users and groups: Group3

o Target resources

- Include: All cloud apps

o Access controls

- Grant: Block access

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online.	☐	☐
User2 will be prevented from signing in to Microsoft SharePoint Online.	☐	☐
User3 will be prevented from signing in to Microsoft SharePoint Online.	☐	☐

Question: 246(Document was last saved: Just now)**HOTSPOT**

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains three users named User1, User2 and User3.

You have the devices shown in the following table.

Name	Platform	Description
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	<i>None</i>
Device3	Android	Microsoft Entra registered

You deploy a virtual machine that has the following configurations:

- Name: VM1
- Resource group: RG1
- Operating system: Windows Server
- Login with Microsoft Entra ID: Enabled

You have the Azure role assignments shown in the following table.

User	Role	Scope
User1	Virtual Machine Local User Login	RG1
User2	Virtual Machine User Login	RG1
User3	Virtual Machine Administrator Login	Sub1

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 sign in to VM1 from Device1 by using their Microsoft Entra credentials.	☐	☐
User2 can sign in to VM1 from Device2 by using their Microsoft Entra credentials.	☐	☐
User3 can sign in to VM1 from Device3 by using their Microsoft Entra credentials.	☐	☐

Question: 247

HOTSPOT

Document was last saved: Just now

You have an Azure subscription that contains two resource groups named RG1 and RG2, a storage account named storage1.

You assign roles for the subscription as shown in the following table.

User	Role
User1	Reader
User2	Reader
User3	Reader
User4	Owner

You assign roles for RG1 as shown in the following table.

User	Role
User1	Reader and Data Access
User2	Contributor

You assign roles for storage1 as shown in the following exhibit.

```
1 [
2   {
3     "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
4     "Scope": "/subscriptions/7fe6d66e-8694-4b54-beae-17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1"
5   }
6 ]
```

You assign roles for storage1 as shown in the following exhibit.

```
1 [
2   {
3     "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
4     "Scope": "/subscriptions/7fe6d66e-8694-4b54-beae-
17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1",
5     "DisplayName": "User3",
6     "SignInName": "User3@contoso.com",
7     "RoleDefinitionName": "User Access Administrator",
8     "RoleDefinitionId": "/subscriptions/7fe6d66e-8694-4b54-beae-
17fd819d4873/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
9     "ObjectId": "919948b2-bc93-41a0-9562-9399576cc8f0",
10    "ObjectType": "User",
11    "RoleAssignmentDescription": "",
12    "ConditionVersion": "",
13    "Condition": ""
14  }
15 ]
```

Roles are NOT assigned for other Azure resources.

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 read the data stored in storage1.	☐	☐
User2 can create a virtual network in RG2.	☐	☐
User3 can assign roles for storage1.	☐	☐

Question: 253

HOTSPOT

You have a Microsoft Entra tenant that contains 1,000 users. The users are assigned Microsoft Entra Suite licenses.

You perform the following actions:

- Deploy Global Secure Access.
- Create a Global Secure Access security profile named Profile1.
- Create the following Conditional Access policies:
 - oName: CAPolicy1
 - oTarget resources: All internet resources with Global Secure Access
 - oName: CAPolicy2
 - oSession:

-Use Global Secure Access security profile: Profile1

To which Global Secure Access traffic forwarding profiles is CAPolicy1 linked, and to which profile does Profile1 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

CAPolicy1 is linked to:

Microsoft traffic profile and Internet access profile

Microsoft traffic profile and Private access profile

Private access profile and Internet access profile

Profile1 applies to:

Internet access profile

Microsoft traffic profile

Private access profile

Question: 254

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains 500 Windows 11 devices.

You have a Microsoft 365 subscription that syncs with the domain.

You create a Conditional Access policy named Policy1.

You need to meet the following requirements:

- Apply Policy1 to all the Windows devices.
- Assess the compliance of the Windows devices with Policy1.

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

NOTE: Each correct selection is worth one point.

Answer Area

Apply Policy1 to all the Windows devices:

- Microsoft Entra hybrid join the devices to the subscription.
- Microsoft Entra join the devices to the subscription.
- Microsoft Entra register the devices to the subscription.

Assess the compliance of the Windows devices with Policy1:

- Enroll the devices in Microsoft Intune.
- Onboard the devices to Microsoft Defender for Endpoint.
- Onboard the devices to Microsoft Purview.

Question: 256

HOTSPOT

You have a Microsoft Entra tenant that contains two remote networks named RemoteNetwork1 and RemoteNetwork2 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1
User3	Group2

You have the devices shown in the following table.

Name	Global Secure Access client	User	Connected to
Device1	Deployed	User1	RemoteNetwork1
Device2	Not deployed	User2	RemoteNetwork1
Device3	Deployed	User3	RemoteNetwork2

You have a Conditional Access policy that has the following settings:

oName: CAPolicy1

oAssignments

-Users: Group1, Group2

-Target resources: All internet resources with Global Secure Access

oAccess controls

-Grant: Require multifactor authentication

oEnable policy: On

Global Secure Access traffic forwarding is configured as shown in the following exhibit.

... > Remote network > Traffic forwarding >

Edit an assignment (Microsoft traffic profile)



Traffic forwarding



Traffic profile

Traffic forwarding

[Refresh](#) | [Got feedback?](#)

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward users running the Global Secure Access client. For cli
[Learn more](#)

One or more profiles are configured and ready to

☒ Microsoft traffic profile

Enabled

Last modified on 01/09/2025, 03:34 PM

☐ Applies to

Internet traffic to Microsoft services

☐ Microsoft traffic policies

4 policies [View](#)

☐ Linked Conditional Access policies

1 policy [View](#)

☐ User and group assignments

0 users, 1 groups assigned [View](#)

☐ Remote network assignments

1 assigned remote networks [Edit](#)

Traffic profile

[+ Add assignments](#)

Name	Assignment type
RemoteNetwork1	Remote networks

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



LIVEWORKSHEETS

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
When User1 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).	☐	☐
When User2 signs in to Microsoft SharePoint Online, the user will be prompted for multifactor authentication (MFA).	☐	☐
When User3 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).	☐	☐

Question: 257**HOTSPOT**

You have a Microsoft Entra tenant named contoso.com that contains a user named User1. User1 has the devices shown in the following table:

Name	Platform	Registered in contoso.com
Device1	Windows 11	Yes
Device2	Windows 11	No
Device3	iOS	Yes

On November 5, 2025, you create and enforce terms of use in contoso.com that has the following settings:

- Name: Terms1
- Display name: Contoso terms of use

- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2025
- Frequency: Monthly

On November 15, 2025, User1 accepts Terms1 on Device3.

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

NOTE: Each correct selection is worth one point.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On November 20, 2025, User1 can accept Terms1 on Device1.	☐	☐
On December 11, 2025, User1 can accept Terms1 on Device2.	☐	☐
On December 7, 2025, User1 can accept Terms1 on Device3.	☐	☐

Question: 263

HOTSPOT -

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.

You deploy Azure AD Connect by using the Express Settings.

You need to configure self-service password reset (SSPR) to meet the following requirements:

▫ When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.

▫ Passwords must be synced between the tenant and the domain regardless of where the password was reset.

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

From the Password reset blade in the Azure Active Directory admin center, configure:

	▼
Authentication methods	
Notifications	
Properties	
Registration	

From Azure AD Connect, enable:

	▼
Federation with Active Directory Federation Services (AD FS)	
Pass-through authentication	
Password hash synchronization	
Password writeback	

Question: 264

HOTSPOT -

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).

You need to receive an alert if a registered application gains read and write access to the users' email.

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

Tool to use:

	▼
Azure AD Identity Protection	
Identity Governance	
Microsoft Cloud App Security	
Microsoft Endpoint Manager	

Policy type to create:

	▼
App discovery	
App protection	
Conditional access	
OAuth app	
Sign-in risk	
User risk	