Question: 361 CertyIQ

HOTSPOT

-

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

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
Admin3	Directory Writer
User1	*None*

The tenant contains a standalone workgroup computer named Computer1 that runs Window 11. Computer1 contains the local users shown in the following table.

Name	Member of
UserA	Administrators
UserB	Power Users
UserC	Device Owners
UserD	Users

Computer1 needs to be joined to contoso.com.

Which local users can join Computer1 to contoso.com, and the Microsoft Entra credentials of which user can be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Local users:

- UserA only
- UserA or UserB only
- UserA or UserC only
- UserA, UserB, or UserC only
- UserA, UserB, UserC, or UserD

Credentials of:

- Admin1 only
- Admin1 or Admin2 only
- Admin1 or Admin3 only
- Admin1, Admin2, or Admin3 only
- Admin1, Admin2, Admin3, or User1

Question: 362 CertyIQ

HOTSPOT

-

You have a Microsoft Entra tenant named contoso.com that contains the dynamic membership groups shown in the following table.

Name	Dynamic membership rule
Group1	(device.displayName -startsWith "Dev") or (device.deviceOSType -eq "Android")
Group2	(device.deviceTrustType -eq "workplace")
Group3	(device.deviceTrustType -eq "AzureAD") and (device.deviceOSType -eq "Android")

You add devices to contoso.com as shown in the following table.

Name	Platform	Join type
Device1	Windows	Microsoft Entra joined
Device2	Windows	Microsoft Entra registered
Phone1	Android	Microsoft Entra registered

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is a member of Group1 only.	○	○
Device2 is a member of Group1 and Group2.	○	○
Phone1 is a member of Group1 and Group3.	○	○

Question: 365

CertyIQ

HOTSPOT
-
You have a Microsoft 365 E5 subscription.
The subscription contains users that have devices onboarded to Microsoft Defender for Endpoint. Defender for Endpoint is configured to forward signals to Microsoft Defender for Cloud Apps.
Cloud Discovery identifies a risky web app named App1.
You need to block users from connecting to App1 from Microsoft Edge. Users must be able to bypass the restriction.
Which type of app tag should you use, and what should you configure to integrate Defender for Endpoint with Defender for Cloud Apps? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

App tag type:

- Monitored
- Sanctioned
- Unsanctioned

Integrate by configuring:

- Anonymization
- Asset rule management
- Enforce app access

Question: 368

CertyIQ

HOTSPOT
-
You have a Microsoft 365 E5 subscription.
You need to use Microsoft Graph PowerShell to assign a Microsoft 365 E5 license to a new user named .
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

```
$e5Sku = [                    ▼]  -All | Where SkuPartNumber -eq 'SPE_E5'
```

- Get-MgSubscribedSku
- Get-MgSubscription
- Get-MgUserLicenseDetail
- Get-MgUserLicenseDetailCount

```
[                             ▼]  -UserId "user1@contoso.com" -AddLicenses @{SkuId = $e5Sku.SkuId} -RemoveLicenses @()
```

- Set-MgUserLicense
- Update-MgSubscriberSku
- Update-MgSubscription

Question: 369 CertyIQ

HOTSPOT
-
You have a Microsoft 365 E5 subscription.
You plan to create a Conditional Access policy named Policy1.
You need to ensure that only Passwordless MFA authentication methods are used when administrators attempt to access the Azure portal, Azure PowerShell, or Azure Command-Line Interface (CLI).
How should you configure Policy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Access controls:

- Set Grant to Require authentication strength.
- Set Grant to Require multifactor authentication.
- Set Session to Use app enforced restrictions.
- Set Session to Use Conditional Access App Control.

Target resources:

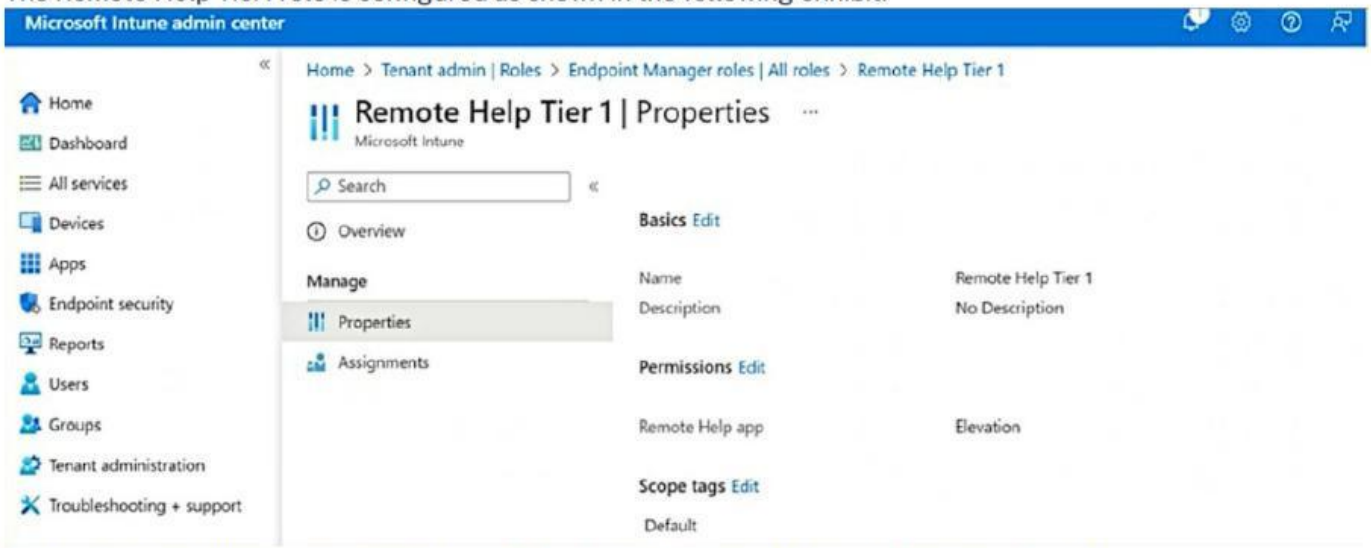
- Azure Credential Configuration Endpoint Service
- Windows Azure Service Management API
- Windows Cloud Login

Name	Platform
Device1	Windows 11
Device2	iOS
Device3	Android

The subscription contains the users shown in the following table.

Name	Role	Role type
Admin1	Help Desk Operator	Built-in role
Admin2	Remote Help Tier1	Custom Intune role

The Remote Help Tier1 role is configured as shown in the following exhibit.



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

Statements	Yes	No
Admin1 can take full control of Device2.	○	○
Admin2 can take full control of Device1.	○	○
Admin2 can take unattended control of Device3.	○	○