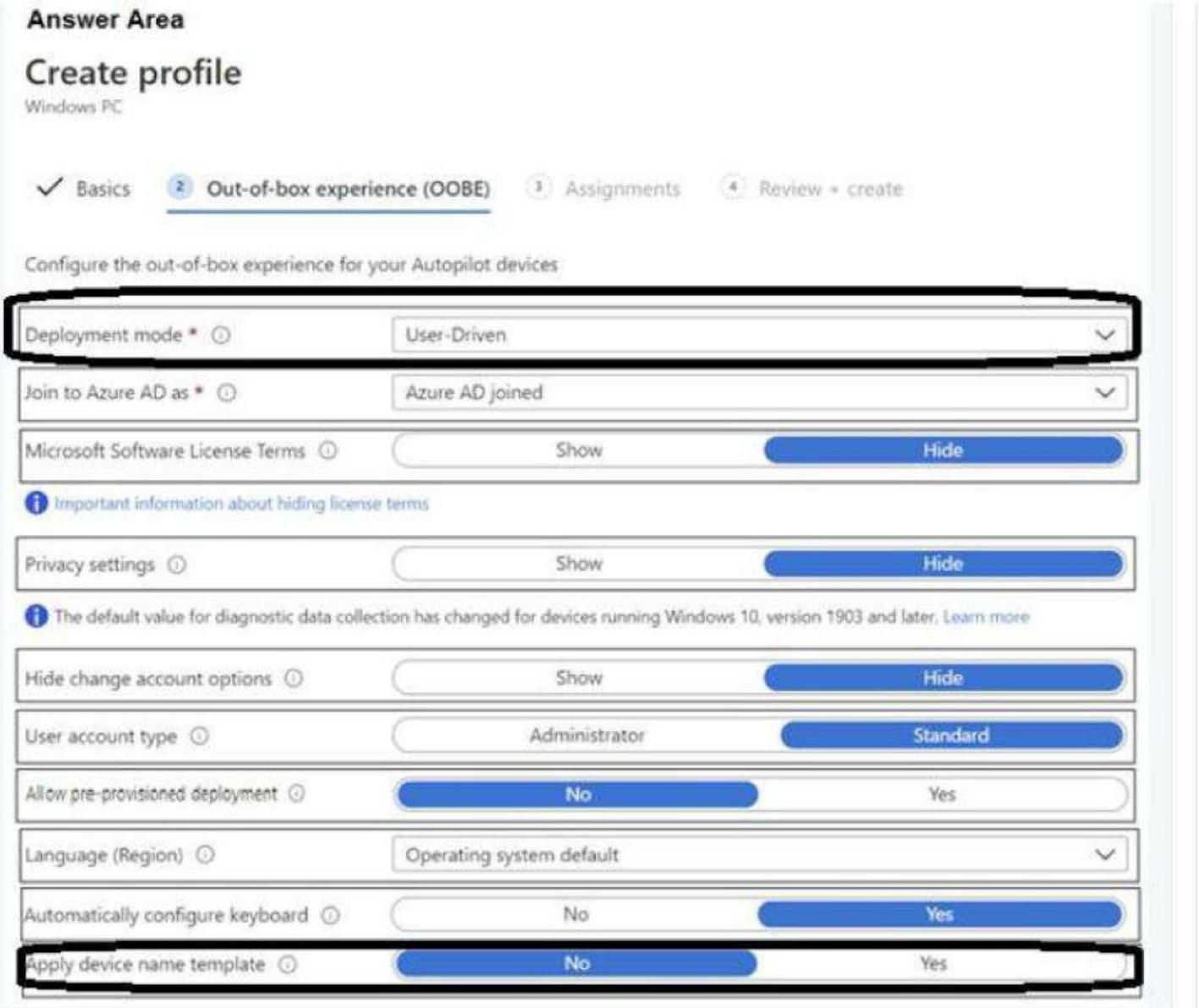
Answer Area



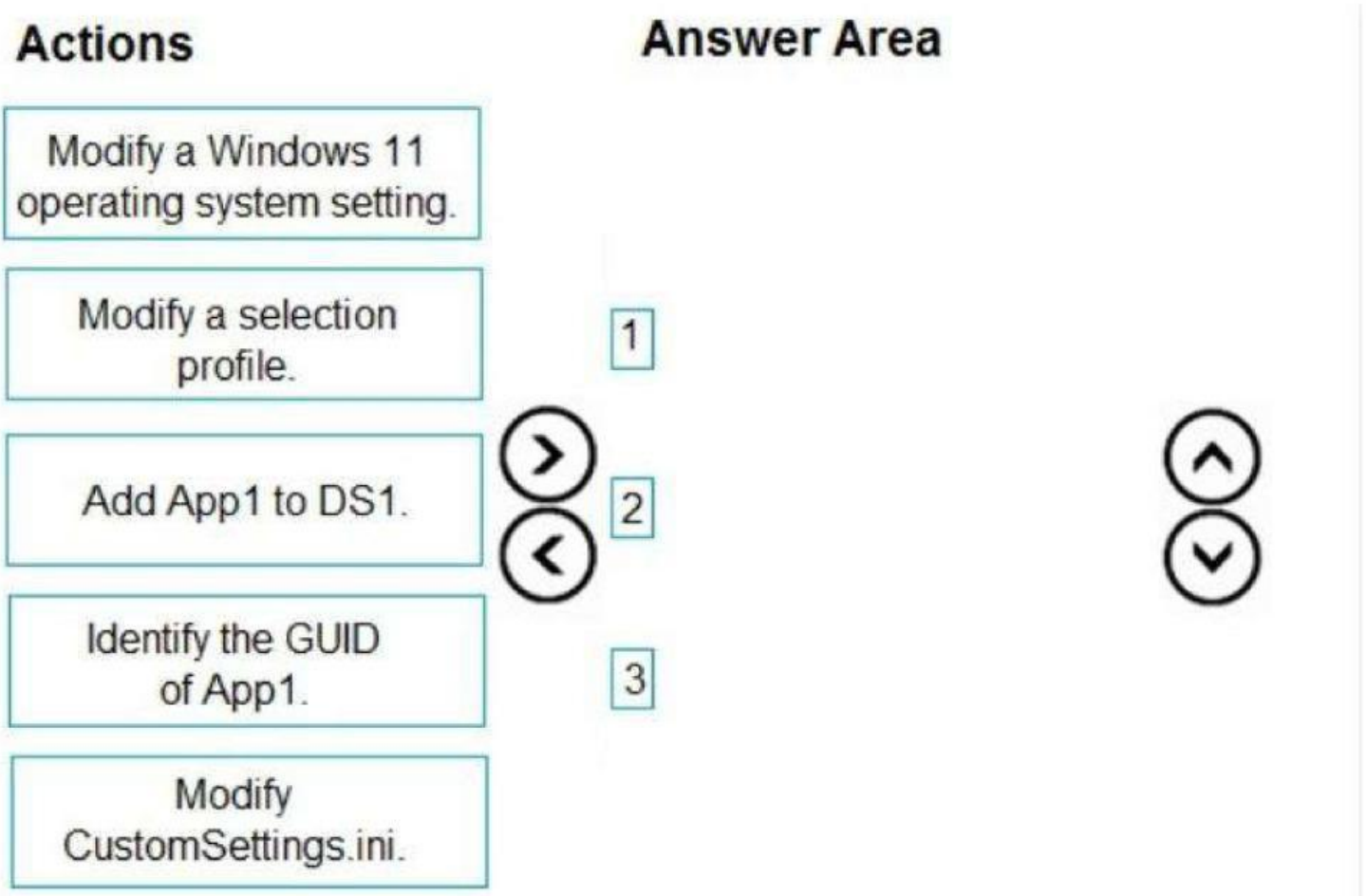
The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	Group3

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 establish a Remote Desktop session to Computer2.	○	○
User2 can establish a Remote Desktop session to Computer2.	○	○
User3 can establish a Remote Desktop session to Computer2.	○	○



Question: 122

CertyIQ

HOTSPOT

-

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Server1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Windows 10 and later

✓ Basics (2) Configuration settings (3) Assignments (4) Applicability Rules (5) Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization
- Printer
- Privacy
- Projection

Previous Next

Answer Area

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Question: 133 CertyIQ

DRAG DROP

-

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.
You need to create Endpoint security policies to enforce the following requirements:
•Computers that run macOS must have FileVault enabled.
•Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
•Computers that run Windows 10 must have Microsoft Defender Application Control enabled.
Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Features

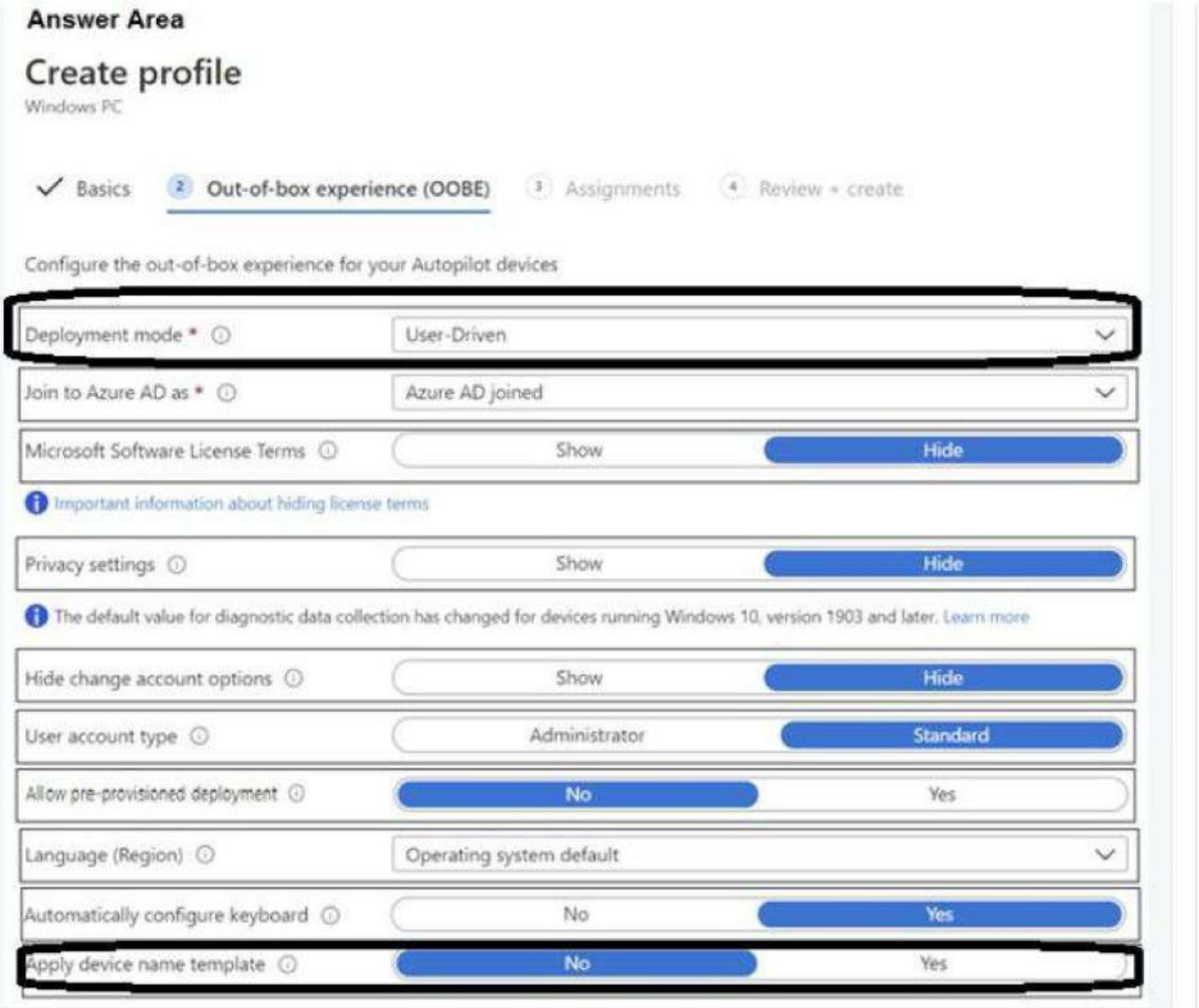
- Account protection
- Attack surface reduction (ASR)
- Disk encryption
- Endpoint detection and response (EDR)

Answer Area

Computers that run macOS must have FileVault enabled:	
Computers that run Windows 10 must have Microsoft Defender Application Control enabled:	
Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:	

Answer:

Answer Area



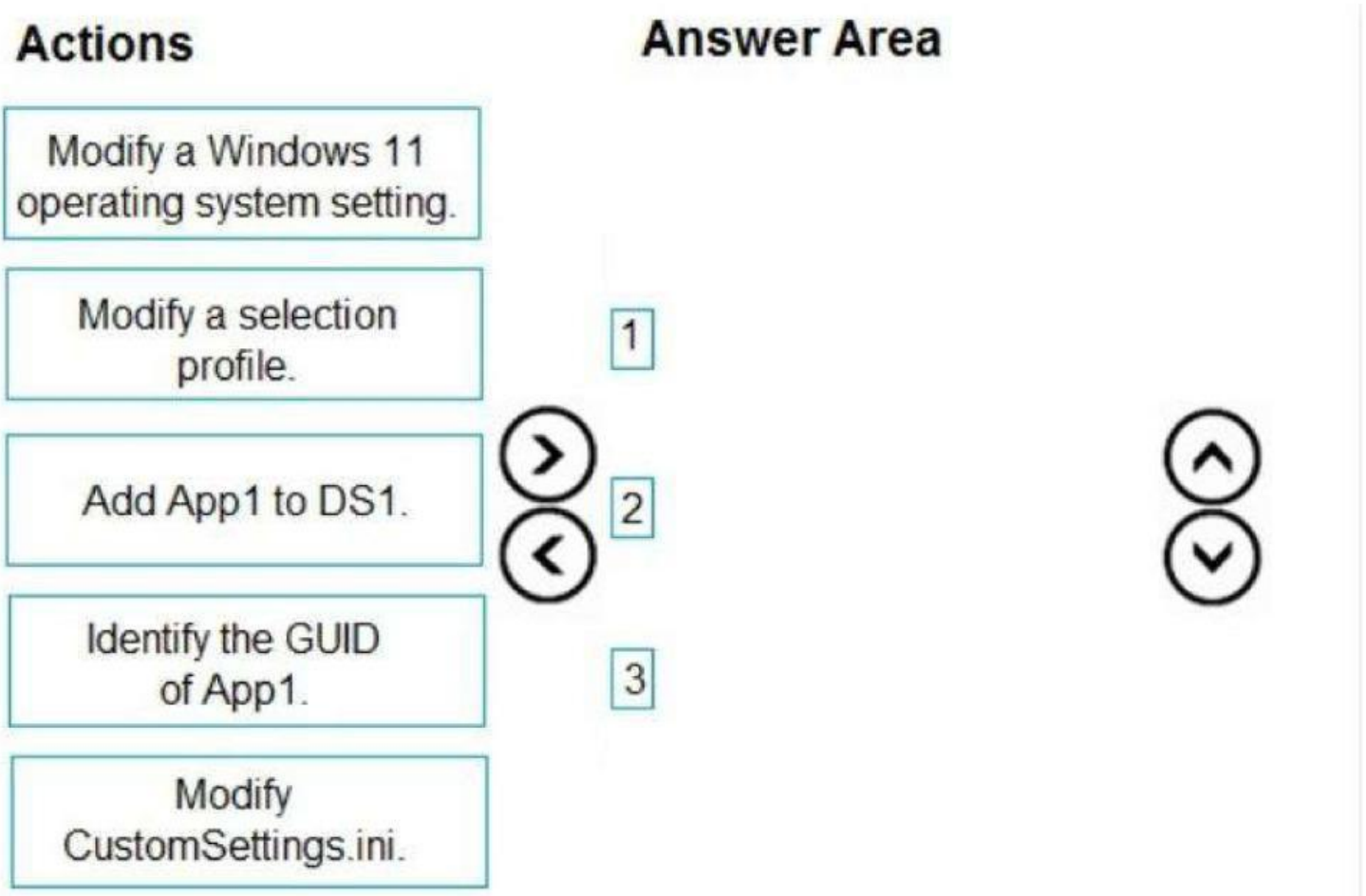
The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	Group3

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 establish a Remote Desktop session to Computer2.	○	○
User2 can establish a Remote Desktop session to Computer2.	○	○
User3 can establish a Remote Desktop session to Computer2.	○	○



Question: 122

CertyIQ

HOTSPOT

-

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Server1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Windows 10 and later

✓ Basics (2) Configuration settings (3) Assignments (4) Applicability Rules (5) Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization
- Printer
- Privacy
- Projection

Previous Next

Answer Area

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Question: 133 CertyIQ

DRAG DROP

-

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.
You need to create Endpoint security policies to enforce the following requirements:
•Computers that run macOS must have FileVault enabled.
•Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
•Computers that run Windows 10 must have Microsoft Defender Application Control enabled.
Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Features

- Account protection
- Attack surface reduction (ASR)
- Disk encryption
- Endpoint detection and response (EDR)

Answer Area

Computers that run macOS must have FileVault enabled:	
Computers that run Windows 10 must have Microsoft Defender Application Control enabled:	
Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:	

Answer:

Answer Area

Identified by Intune as a personal device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4