Connect from:

- Computer1 only
- Computer1 and Computer2 only
- Computer1 and Computer3 only
- Computer1, Computer2, Computer3, and Computer4

Manage:

- Computer1 only
- Computer1 and Computer2 only
- Computer1 and Computer3 only
- Computer1, Computer2, and Computer4 only
- Computer1, Computer2, Computer3, and Computer4

You need to deploy a compliance solution that meets the following requirements:
•Marks the devices as Not Compliant if they do not meet compliance policies
•Remotely locks noncompliant devices
What is the minimum number of compliance policies required, and which devices support the remote lock action?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of compliance policies required:

- 1
- 2
- 3
- 4
- 5

Devices that support the remote lock action:

- Device1 only
- Device2 and Device3 only
- Device4 and Device5 only
- Device2, Device3, Device4, and Device5
- Device1, Device2, Device3, Device4, and Device5

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.
You have a Microsoft 365 E5 subscription that includes Microsoft Intune and syncs with the AD DS domain.
Windows Local Administrator Password Solution (Windows LAPS) is enabled in Microsoft Entra ID.
The subscription has the custom roles shown in the following table.

Name	Permission
Role1	microsoft.directory/deviceLocalCredentials/password/read
Role2	microsoft.directory/deviceLocalCredentials/standard/read
Role3	microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceLocalCredentials/password/read

Microsoft Entra contains the users shown in the following table.

Name	Built-in role	Assigned custom roles
User1	Helpdesk Administrator	Role1
User2	Security Reader	Role2
User3	*None*	Role3

You have the devices shown in the following table.

Name	Domain Join Type
Device1	Joined to AD DS
Device2	Microsoft Entra hybrid joined
Device3	Microsoft Entra joined

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 use Microsoft Entra to read the local administrator password of Device1.	○	○
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	○
User3 can use Microsoft Entra to read the local administrator password of Device3.	○	○

Question: 285

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription and use Microsoft Intune.
You purchase 50 Windows devices.
You configure automatic enrollment to Intune for Microsoft Entra joined devices.
You need to use a provisioning package to join the devices to Microsoft Entra.
What should you use to create the provisioning package, and what is the maximum amount of time you can use the package for bulk enrollment? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Use:

- Intune Company Portal
- Microsoft Deployment Toolkit (MDT)
- Windows Configuration Designer
- Windows Setup

Maximum amount of time:

- 30 days
- 90 days
- 180 days
- 365 days

Question: 287

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You need to route Microsoft Intune logs to an Azure resource that supports the use of visuals, monitoring, and alerting.

Which settings should you configure in Intune, and which resource should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Settings:

- Connectors and tokens
- Device diagnostics
- Diagnostic settings
- Intune add-ons

Resource:

- A Log Analytics workspace
- An Azure logic app
- A storage account
- A virtual machine

Answer Area

Require jailbroken devices to be marked as noncompliant:

- Device Health
- Device Properties
- System Security

Require a password to unlock mobile devices:

- Device Health
- Device Properties
- System Security

Question: 290

CertyIQ

HOTSPOT

-

You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.
You have a device group named Group1 that contains five Windows 11 devices.
You need to ensure that the devices in Group1 automatically receive new Windows 11 builds before the builds are released to the public.
What should you configure in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Profile type:

- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later
- Update rings for Windows 10 and later

Prerelease channel:

- Beta Channel
- Dev Channel
- Windows Insider -
- Release Preview

Name	Join type	Enrolled in Intune
Device1	Joined to the AD DS domain	Yes
Device2	Microsoft Entra hybrid joined	Yes
Device3	Microsoft Entra joined	No

You have an Endpoint security policy that is configured as shown in the following table.

Setting	Value
Name	Policy1
Platform	Windows 10 and later
Profile	Local admin password solution (Windows LAPS)
Backup Directory	Backup the password to Azure AD only
Password Age Days	30
Assignments	Include: All devices

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
The local administrator password of Device1 will be reset every 30 days.	○	○
The local administrator password of Device2 will be recoverable from Microsoft Entra ID.	○	○
The local administrator password of Device3 will be reset every 30 days.	○	○

Answer Area

App1:

- A Required assignment to a device group
- A Required assignment to a user group
- An Available assignment to a device group
- An Available assignment to a user group

App2:

- A Required assignment to a device group
- A Required assignment to a user group
- An Available assignment to a device group
- An Available assignment to a user group

Answer Area

Statements	Yes	No
Azure Monitor collects CPU performance data from Device1.	○	○
Azure Monitor collects memory performance data from Device2.	○	○
Azure Monitor collects CPU performance data from Device3.	○	○