DUMPSBOSS.

# Endpoint Administrator

## Microsoft MD-102

## Version Demo

**Total Demo Questions: 66**

**Total Premium Questions: 680**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Deploy Windows client | 131 |
| Topic 2, Manage identity and compliance | 192 |
| Topic 3, Manage, maintain, and protect devices | 222 |
| Topic 4, Manage applications | 87 |
| Topic 5, Case Study Contoso, Ltd. | 36 |
| Topic 6, Case Study Litware inc | 12 |
| Total | 680 |

QUESTION NO: 1

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have 300 Android Enterprise fully managed devices.

You need to allow users to access a corporate web application from Microsoft Edge. The web application must be available from the managed home screen without requiring users to enter the URL.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Add a web link app in Intune.

**B.** Assign the web link app to the device group as Required.

**C.** Create an Android app configuration policy.

**D.** Create a compliance policy.

**E.** Approve the web application in Managed Google Play.

**ANSWER: A B**

**Explanation:**

**Add a web link app in Intune** creates an application entry that points to the corporate web application. Web links can be deployed to supported Android Enterprise devices and provide users with a managed shortcut to the specified site.

**Assign the web link app to the device group as Required** ensures that the shortcut is deployed automatically to the fully managed devices. With the managed home screen configuration in use, the assigned web link can be made available to users as an approved application entry.

An Android app configuration policy configures an app but does not create a web shortcut. A compliance policy evaluates device state, and a managed Google Play approval is used to acquire Android applications rather than web links. For more information, see Web links in Microsoft Intune.

**QUESTION NO: 2**

Which users can create a new group on Computer3?

**A.** User31 only

**B.** User1 and User32 only

**C.** Admin1 and User31 only

**D.** Admin1, User31, and User32 only

**ANSWER: C**

**Explanation:**

Admin1 and User31 only can create a new local group on Computer3 because creating and managing local security groups is an administrative action on a Windows device. Local groups are stored in the device's local Security Accounts Manager database, and the ability to change them is controlled by local administrative permissions. In the stated configuration, Admin1 and User31 have the required local administrator privileges on Computer3, whereas the remaining listed users do not have permission to administer the local group database.

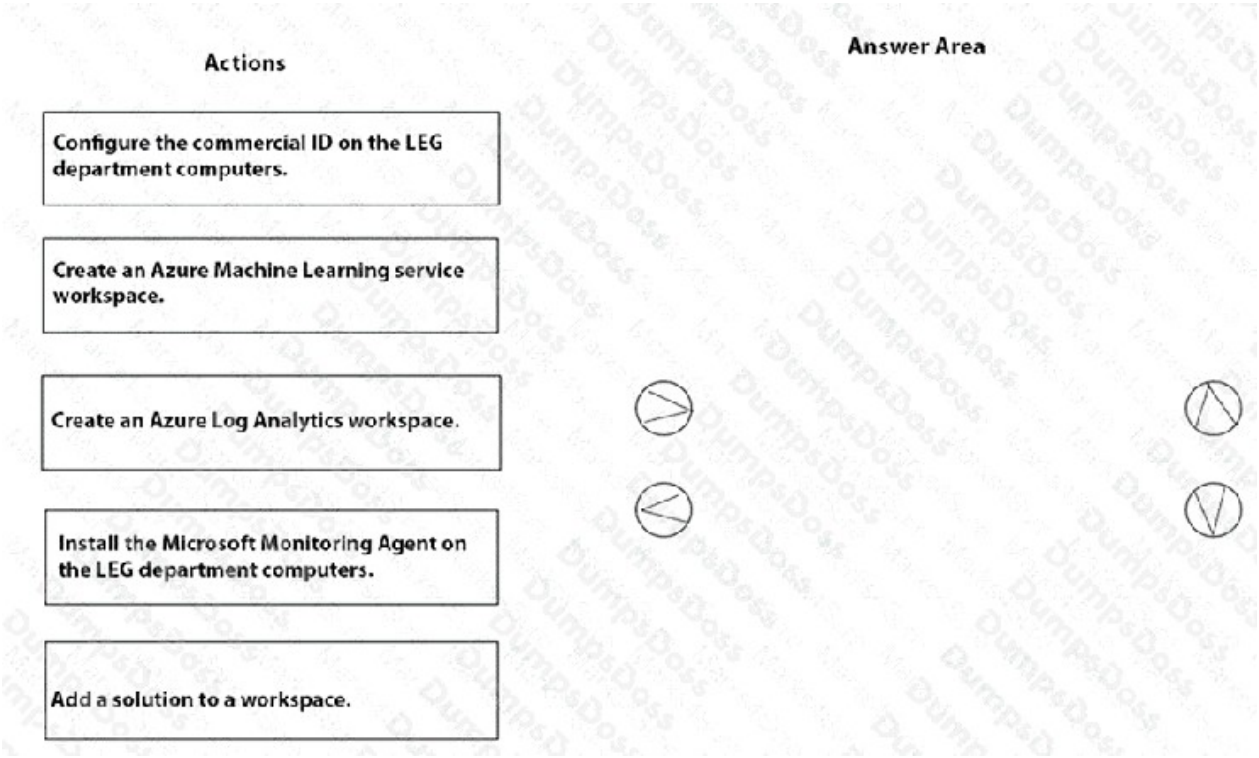
On Microsoft Entra joined devices, a user assigned local administrator rights can perform administrative tasks such as managing local users and groups. Microsoft Entra roles and device-join configuration can also determine who is placed in the local Administrators group, but only users who ultimately receive local administrator permissions on the specific device

can create the new group. Microsoft documents the mechanisms for assigning local administrator access to Microsoft Entra joined devices and the security role of local accounts and groups. See Manage local administrators on Microsoft Entra joined devices and Local accounts.

## QUESTION NO: 3 - (DRAG DROP)

You need to meet the technical requirements for the LEG department computers.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.




## ANSWER:

**Explanation:**

The correct sequence is to create an Azure Log Analytics workspace, add a solution to that workspace, and then configure the commercial ID on the LEG department computers. A Log Analytics workspace is the Azure resource that provides the data location and service context for this Windows Analytics-era onboarding workflow. It must exist before a solution can be enabled, because the solution is associated with a specific workspace rather than being deployed independently to endpoints.

After the workspace is available, adding the solution enables the relevant analytics service in that workspace. This service setup produces the tenant/workspace association information used for endpoint enrollment. Once the solution has been connected to the workspace, the commercial ID can be obtained for that configured service instance.

The final step is applying that commercial ID to the LEG computers. The commercial ID identifies the organization's analytics configuration and lets Windows diagnostic data from those devices be associated with the correct Azure workspace and enabled solution. It can be deployed to managed Windows devices through policy, including Group Policy or Microsoft Endpoint Manager policy, as appropriate for the organization's management model.

This order ensures the cloud-side destination and solution are completely established before devices are pointed to them. Microsoft's Windows deployment documentation describes the use of a Log Analytics workspace and solutions for Windows analytics services, while Microsoft's policy documentation covers configuring the Commercial ID used by enterprise Windows devices. See Set up Windows Analytics in the Azure portal and Policy CSP - System: EnableCommercialID.

## QUESTION NO: 4

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

| Name | Memory | TPM |
|---|---|---|
| Device1 | 16 GB | *None* |
| Device2 | 8 GB | Version 1.2 |
| Device3 | 4 GB | Version 2.0 |

Which devices can be configured by using Windows Autopilot self-deploying mode?

**A.** Device2 only

**B.** Device3 only

**C.** Device1 and Device3 only

**D.** Device1, Device2, and Device3

## ANSWER: B

**Explanation:**

**Device3 only** is correct. Windows Autopilot self-deploying mode is designed for shared, kiosk, and other userless deployment scenarios. Unlike user-driven Autopilot, the process does not require a user to provide Microsoft Entra credentials during the out-of-box experience. Instead, the device uses TPM-based device attestation to establish its identity and securely complete Microsoft Entra join and Intune enrollment.

Consequently, a device used with this mode must meet the self-deploying prerequisites, including a supported physical Windows device, Windows 10 version 1809 or later, TPM 2.0, and support for TPM 2.0 device attestation. It must also be registered with the Windows Autopilot service and assigned a self-deploying Autopilot deployment profile. Based on the properties shown in the device table, Device3 is the device that meets these requirements and can therefore use self-deploying mode.

Microsoft documents the TPM 2.0 attestation dependency and deployment behavior in Windows Autopilot self-deploying mode. See also the applicable operating system, Microsoft Entra ID, Intune, and hardware prerequisites in Windows Autopilot requirements.

## QUESTION NO: 5

You have a Microsoft 365 subscription that uses Microsoft Intune and Microsoft Entra ID.

You have 500 Windows 11 devices enrolled in Intune.

You need to ensure that users can access Microsoft 365 services only from devices that meet your organization's compliance requirements.

Which two policies should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** a compliance policy

**B.** a Conditional Access policy that requires a device to be marked as compliant

**C.** an app configuration policy

**D.** an enrollment restriction

**E.** an endpoint security antivirus policy

**ANSWER: A B**

**Explanation:**

A **compliance policy** defines the device requirements that Intune evaluates, such as minimum operating-system version, encryption status, password requirements, and device-threat level. Intune reports the resulting compliance state to Microsoft Entra ID.

A **Conditional Access policy that requires a device to be marked as compliant** uses that reported compliance state as an access control. When a user attempts to access the selected cloud applications, Microsoft Entra ID allows the connection only when the device is compliant. Both policies are required: the compliance policy evaluates the device, and Conditional Access enforces the access requirement. See Create a compliance policy in Microsoft Intune and Require compliant or hybrid Microsoft Entra joined devices with Conditional Access.

## QUESTION NO: 6

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to deploy Windows Autopilot devices by using Microsoft Entra hybrid join.

Which two components are required to support the deployment? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Microsoft Entra Connect

**B.** The Intune Connector for Active Directory

**C.** An on-premises Exchange Server

**D.** A Microsoft Deployment Toolkit deployment share

**E.** Windows Server Update Services (WSUS)

**ANSWER: A B**

**Explanation:**

**Microsoft Entra Connect** is required to synchronize the on-premises Active Directory environment with Microsoft Entra ID for a hybrid identity deployment. The hybrid join configuration requires device-related synchronization and the appropriate service connection point configuration so that domain-joined devices can register with Microsoft Entra ID.

**The Intune Connector for Active Directory** is required for the Autopilot Microsoft Entra hybrid join deployment flow. Intune uses the connector to request an offline domain join blob for each device. The connector must have the delegated permissions required to create the computer account in the target organizational unit.

An on-premises Exchange server and a Microsoft Deployment Toolkit deployment share are not required for this Autopilot deployment method. For more information, see Windows Autopilot Microsoft Entra hybrid join.

## QUESTION NO: 7

Your on-premises network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

The domain contains a domain controller named dc1.contoso.com.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune Suite.

You have an Azure subscription that contains the resources shown in the following table.

| Name | Description |
|---|---|
| LNG1 | Local network gateway that uses the public IP address of the local infrastructure |
| GW1 | Virtual network gateway |
| GW2 | Virtual network gateway |
| CN1 | Site-to-Site (S2S) VPN connection that connects LNG1 and GW1 |

The subscription contains the virtual networks shown in the following table.

| Name | IP address space | Subnet | DNS configuration | Virtual network gateway |
|---|---|---|---|---|
| VNet1 | 192.168.10.0/24 | 192.168.10.0/26 | dc1.contoso.com | GW1 |
| VNet2 | 192.168.11.0/24 | 192.168.11.0/26 | Azure DNS | *None* |
| VNet3 | 192.168.12.0/24 | 192.168.12.0/26 | Azure DNS | GW2 |

You plan to deploy Windows 365 Enterprise Cloud PC.

You need to create an Azure network connection (ANC) that will use Microsoft Entra hybrid join.

Which virtual network can you use for the ANC?

**A.** VNet1 only

**B.** VNet2 only

**C.** VNet3 only

**D.** VNet1 and VNet2

**E.** VNet1 and VNet3

**ANSWER: A**

**Explanation:**

**VNet1 only** is correct. A Windows 365 Enterprise Azure network connection using Microsoft Entra hybrid join places Cloud PCs into a customer-managed Azure virtual network and must support joining those devices to the on-premises AD DS domain. Consequently, the selected network must have line-of-sight connectivity to a writable domain controller for contoso.com, including dc1.contoso.com, and must use DNS that can resolve the AD DS domain and domain-controller records. This connectivity is required during provisioning so that the Cloud PC can locate the domain, authenticate the domain-join operation, and communicate with the required AD DS services.

Based on the network details provided, VNet1 is the virtual network that meets the hybrid-join connectivity and DNS prerequisites for the on-premises contoso.com environment. It can therefore be selected for the Azure network connection used by the Windows 365 Enterprise provisioning policy. Azure network connections are specifically intended for scenarios in which Cloud PCs require access to on-premises resources, and Microsoft Entra hybrid join requires access to the organization's AD DS infrastructure. For the applicable configuration requirements, see Azure network connections for Windows 365 and Windows 365 network requirements.

**QUESTION NO: 8**

You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.

You create a Conditional Access policy named Policy! that requires multifactor authentication (MFA).

You need to ensure that Policy1 only applies to devices marked as noncompliant. Which settings of Policy1 should you configure?

**A.** Device platforms under Conditions

**B.** Filter for devices under Conditions

**C.** Target resources

**D.** Grant

**E.** Session

**ANSWER: B**

**Explanation:**

**Filter for devices under Conditions** is the appropriate setting because Conditional Access device filters let an administrator include or exclude devices dynamically based on device attributes. For an Intune-enrolled device, the `device.isCompliant` attribute is available to a Conditional Access filter. Configure the filter to include filtered devices and use the rule `device.isCompliant -eq false`. The policy's MFA grant requirement will then be evaluated only when the sign-in originates from a device whose compliance state is noncompliant. Device filters are evaluated as part of Conditional Access policy processing and can be combined with user, application, and other condition assignments. This provides the necessary device-state targeting while retaining the MFA requirement in the policy's grant controls. Microsoft documents the available filter properties, including `device.isCompliant`, and the supported rule syntax in its Conditional Access device filter guidance. See Conditional Access device filters and supported device properties and operators.

**QUESTION NO: 9**

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Enable the Allow Remote Shell access setting.

**B.** Enable the Allow remote server management through WinRM setting.

**C.** Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.

**D.** Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.

**E.** Set the Startup Type of the Remote Registry service to Automatic.

**F.** Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

**ANSWER: B C F**

**Explanation:**

Enabling **Allow remote server management through WinRM** configures the WinRM service to accept remote-management requests and lets the administrator specify the IPv4 and IPv6 address filters from which connections are permitted. This policy is the central WinRM configuration setting when deployment is performed through Group Policy.

Setting the startup type of the **Windows Remote Management (WS-Management)** service to **Automatic** ensures that the WinRM service is available after the computer starts. A listener cannot provide consistent remote management if the underlying service is not started on managed endpoints.

Enabling **Windows Defender Firewall: Allow inbound remote administration exception** supplies the firewall allowance required for inbound remote-administration communications. This complements the WinRM service and listener configuration by ensuring that local firewall policy does not prevent remote management connectivity. Applying these settings through a computer-based Group Policy object enables consistent configuration across all domain-joined Windows 10 devices without requiring an administrator to configure each device manually.

Microsoft's WinRM documentation describes the service, listener, and firewall requirements for remote management: Installation and configuration for Windows Remote Management. For firewall policy deployment and management, see Configure Windows Firewall.

## QUESTION NO: 10

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune.

You need to prevent the printing of corporate data from managed apps on the devices.

What should you configure?

**A.** an app configuration policy

**B.** a security baseline

**C.** an app protection policy

**D.** an iOS app provisioning profile

## ANSWER: C

**Explanation:**

An app protection policy is the appropriate configuration because Intune app protection policies apply data-loss prevention controls directly to supported managed apps on iOS/iPadOS. The requirement concerns corporate data used within managed apps, rather than a device-wide printing restriction, so the control must be applied at the app and data layer. In an iOS/iPadOS app protection policy, the Data protection settings include the *Printing org data* setting. Configuring this setting to block printing prevents users from printing organizational content from apps that are targeted by, and support, the policy.

This approach protects Microsoft 365 corporate content in supported applications while allowing administrators to target the relevant user groups and applications. It is also suitable for both enrolled devices and supported app-protection scenarios where device enrollment is not the primary mechanism for securing organizational data. Microsoft describes app protection policies as controls that help prevent the intentional or accidental disclosure of organizational data at the application level. The iOS/iPadOS policy settings specifically document the printing control for organizational data. See Microsoft Intune app protection policies and iOS/iPadOS app protection policy settings.

## QUESTION NO: 11

Your network contains an Active Directory domain.

You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

**A.** Yes

**B.** No

## ANSWER: B

**Explanation:**

**No** is correct. The successful synchronization status indicates that Microsoft Entra Connect is operating normally for the objects within its configured synchronization scope. When all users except those in one specific organizational unit are missing, the appropriate action is to review and update the Active Directory domain and OU filtering configuration in

Microsoft Entra Connect. OU filtering determines which on-premises Active Directory containers Microsoft Entra Connect imports and processes for synchronization. The OU containing the 10 accounts must be selected in the connector's configuration.

Run the Microsoft Entra Connect wizard, select *Customize synchronization options*, authenticate as required, and update the Domain and OU filtering selection to include the affected OU. After the configuration is applied, run or allow the next synchronization cycle so that the users are imported, synchronized, and exported to Microsoft Entra ID. Microsoft documents OU-based filtering as the supported way to limit or include Active Directory objects based on their organizational-unit location. See Microsoft Entra Connect Sync: Configure filtering and Custom installation of Microsoft Entra Connect.

## QUESTION NO: 12

You need to capture the required information for the sales department computers to meet the technical

requirements.

Which Windows PowerShell command should you run first?

**A.** Install-Module WindowsAutoPilotIntune

**B.** Install-Script Get-WindowsAutoPilotInfo

**C.** Import-AutoPilotCSV

**D.** Get-WindowsAutoPilotInfo

## ANSWER: B

**Explanation:**

`Install-Script Get-WindowsAutoPilotInfo` is the appropriate first command because it installs the PowerShell script that collects Windows Autopilot device-registration data. The Get-WindowsAutopilotInfo script obtains the device hardware hash and relevant identifying information needed to register corporate devices with the Windows Autopilot service. After the script has been installed, an administrator can run it on each applicable computer and export the collected data to a comma-separated values file for import into Intune or the Autopilot device registration process.

This ordering matters operationally: PowerShell must first make the script available on the computer before the script can be invoked to perform collection. The script is distributed through the PowerShell Gallery, and `Install-Script` downloads and installs it for use in the current environment. Microsoft's Autopilot guidance describes using Get-WindowsAutopilotInfo to gather the hardware hash for manual device registration, including scenarios where device information must be collected from existing Windows devices. See Manually register devices with Windows Autopilot and the Get-WindowsAutopilotInfo PowerShell Gallery package.

## QUESTION NO: 13

Your network contains an Active Directory domain named contoso.com. The domain contains named Computer1 that runs Windows 10.

---

| Name | Permission |
|---|---|
| User1 | Full control |
| User2 | Change |

When accessing Share1, which two actions can be performed by User1 but not by User2? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Delete a file created by another user.

**B.** Set the permissions for a file.

**C.** Rename a file created by another user.

**D.** Take ownership of file.

**E.** Copy a file created by another user to a subfolder.

**ANSWER: B D**

**Explanation:**

Set the permissions for a file and Take ownership of file are the actions that User1 can perform exclusively. Access to a folder over SMB is determined by the combination of share permissions and NTFS permissions; the effective access is constrained by the most restrictive permission set. Here, the underlying NTFS folder grants Everyone Full control, so it does not limit either user. The meaningful distinction therefore comes from the permissions applied to Share1.

User1's Full Control share permission includes the security-related rights needed to modify a file's discretionary access control list and to take ownership. Consequently, User1 can change a file's permissions and assign ownership through the shared-folder connection. These capabilities are distinct from ordinary content-management tasks and are available because Full Control includes the rights associated with changing permissions and ownership. Microsoft documents that shared-folder permissions are evaluated together with NTFS permissions for network access, and that Full access is the SMB share access right that provides unrestricted access at the share layer. See Share and NTFS permissions on a file server and Grant-SmbShareAccess.

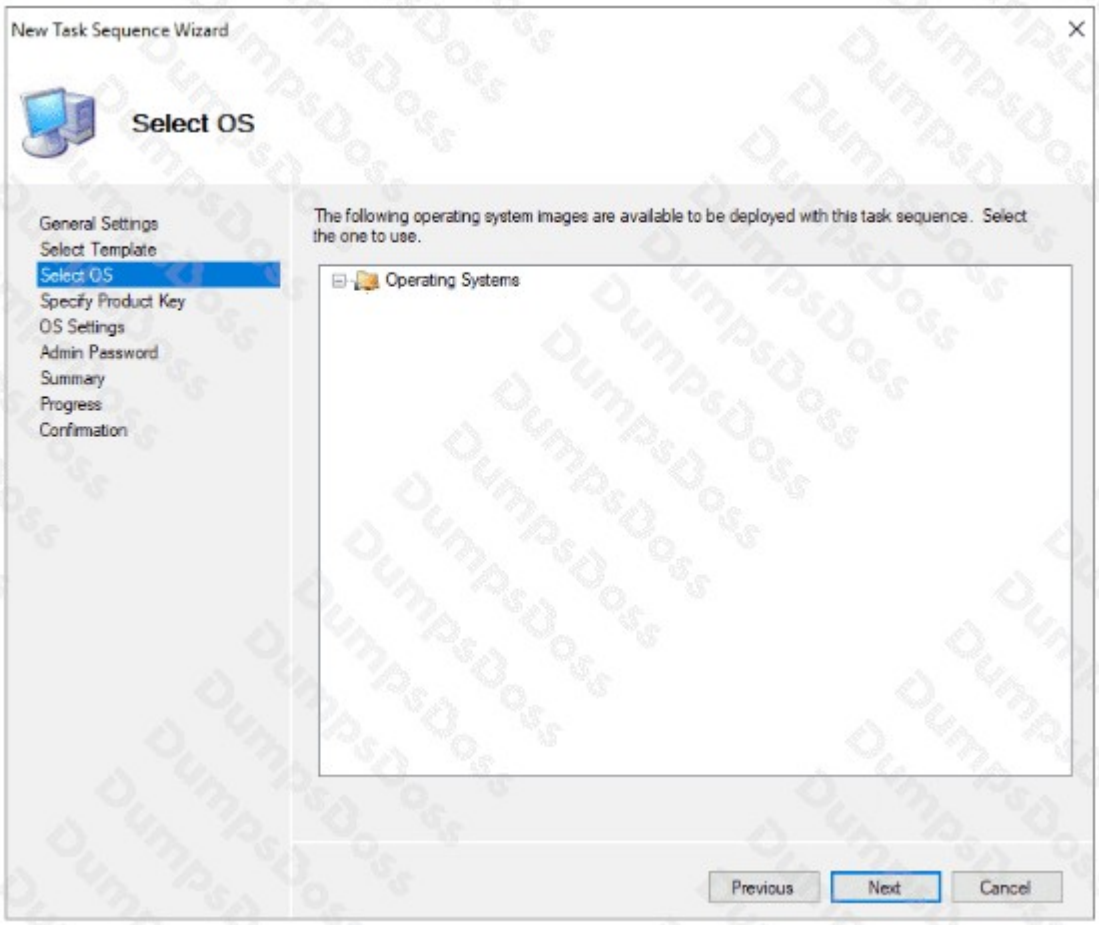
**QUESTION NO: 14**

You have a Microsoft Deployment Toolkit (MDT) deployment share.

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence

template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.




You need to be able to select an operating system image to perform a Windows 11 in-place upgrade.

What should you do?

**A.** Enable monitoring for the deployment share.

**B.** Import a full set of source files.

**C.** Import a custom image file.

**D.** Run the Update Deployment Share Wizard.

**ANSWER: B**

**Explanation:**

**Import a full set of source files.** is correct because an MDT Standard Client Upgrade Task Sequence performs an in-place Windows upgrade by launching Windows Setup from complete installation media. MDT therefore requires an operating system entry that contains the full Windows source structure, including `setup.exe`, the `sources` folder, and the Windows image files. A standalone custom WIM does not provide the setup components required to initiate this type of upgrade.

Mount the Windows 11 ISO, or extract its contents to a folder, and then use the Operating Systems node in Deployment Workbench to import that folder by selecting the full-source-files import method. After the source files are imported successfully, MDT creates an operating system item that can be selected in the New Task Sequence Wizard when creating a Standard Client Upgrade Task Sequence. The task sequence can then use the imported Windows Setup media to retain user data, installed applications, and configuration as supported by the in-place upgrade process.

Microsoft documents importing complete operating system source files into MDT deployment shares and using MDT task sequences for deployment scenarios. See Get started with the Microsoft Deployment Toolkit and Understand MDT task sequences.

## QUESTION NO: 15

Your company has devices enrolled in Microsoft Intune as shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | Android device administrator |
| Device3 | iOS |

In Microsoft Intune admin center, you define the company's network as a location named Location1.

Which devices can use network location-based compliance policies?

**A.** Device1 only

**B.** Device2 only

**C.** Device1 and Device2 only

**D.** Device2 and Device3 only

**E.** Device1, Device2, and Device3

## ANSWER: B

**Explanation:**

Device2 only is correct because network location is a compliance-policy setting supported for Windows 10 and later devices in Intune. The setting enables Intune to evaluate whether the Windows device is connected to a network that matches a network location configured by the organization. Administrators can then use the device's resulting compliance state with Microsoft Entra Conditional Access to control access to organizational resources.

In the device table, Device2 is the device that runs a supported Windows platform for this compliance capability. A network location must first be created in Intune and then selected in a Windows compliance policy assigned to the applicable device or user group. The device evaluates its network connection against that configured location during compliance assessment. This is a device-compliance capability, rather than simply a Conditional Access named-location condition, so the platform support for the Intune compliance setting is decisive. Microsoft documents Network location under the settings available when creating a Windows compliance policy. See Windows compliance settings in Microsoft Intune and Device compliance policies in Microsoft Intune.

## QUESTION NO: 16

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices.

What should you do first?

**A.** Create a configuration profile.

**B.** Add a certificate connector.

**C.** Configure the Partner device management settings.

**D.** Link your managed Google Play account to Intune.

## ANSWER: D

**Explanation:**

Link your managed Google Play account to Intune. Android Enterprise uses managed Google Play as its enterprise app store and app-distribution service. Connecting the Intune tenant to a managed Google Play account is therefore the

foundational setup step before Android Enterprise applications can be approved, synchronized into Intune, assigned, and installed on enrolled devices. The connection establishes the relationship between the organization's Intune service and Google's managed app ecosystem. After it is configured, an administrator can browse or search managed Google Play from the Intune admin center, approve public applications, synchronize those applications so that they appear in Intune, and assign them to relevant user or device groups as required or available. This integration also supports private applications that an organization publishes through managed Google Play for its Android Enterprise users. Microsoft identifies connecting Intune to managed Google Play as part of the required Android Enterprise configuration process, and its Android app-management guidance describes approving and syncing managed Google Play apps before assignment. Review the setup process in Connect Intune to Android Enterprise and the app workflow in Add managed Google Play apps to Intune.

## QUESTION NO: 17

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have 200 corporate-owned iPhone devices.

You need to ensure that the devices are supervised and enroll automatically in Intune when users turn on the devices for the first time.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Add the devices to Apple Business Manager.

**B.** Assign the devices to the Intune MDM server in Apple Business Manager.

**C.** Require users to enroll by using User Enrollment.

**D.** Create managed Apple IDs for all users.

**E.** Create an app protection policy.

## ANSWER: A B

**Explanation:**

**Add the devices to Apple Business Manager** is required to make organization-owned Apple devices available for Automated Device Enrollment. Devices purchased through a participating reseller can be added by the reseller, or eligible devices can be added by using Apple Configurator.

**Assign the devices to the Intune MDM server in Apple Business Manager** directs the devices to Intune during Setup Assistant. Intune can then apply an Automated Device Enrollment profile, which enrolls the devices and places them under supervision.

User enrollment is designed for personally owned devices and does not provide the same organization-owned supervised management model. Apple IDs and app protection policies do not configure automated device enrollment. For more information, see Automatically enroll iOS/iPadOS devices with Apple Business Manager.

## QUESTION NO: 18

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.

You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

**A.** To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.

**B.** To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.

**C.** To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

**D.** To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.

**E.** To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

**F.** To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

**ANSWER: C E**

**Explanation:**

For Windows devices that are Microsoft Entra ID joined and already managed by Intune, centrally deploying Intune device configuration policy minimizes administrative effort. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings. This profile type includes Microsoft Defender Antivirus policy settings, enabling consistent management of antivirus behavior across the assigned device group without configuring each computer individually. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings. The same Endpoint protection profile family supports Microsoft Defender Firewall settings, including enabling the firewall and configuring protection behavior for network profiles. A single cloud-based management service is particularly appropriate here because the devices are already Intune-managed and do not require additional on-premises infrastructure. Policies can be scoped to the relevant device group and are delivered through Intune management, which provides a scalable and low-touch approach for all 100 endpoints. Microsoft documents Intune's support for configuring antivirus policies through endpoint security and configuration policy, as well as centrally managing Windows Firewall settings. See Microsoft Defender Antivirus policy settings in Intune and Firewall policy settings in Intune.

**QUESTION NO: 19**

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Deploy the Remote Help app to Device1.

**B.** Assign the Help Desk Operator role to User1.

**C.** Assign the Intune Administrator role to User1.

**D.** Assign a Microsoft 365 E5 license to User1.

**E.** Rerun device onboarding on Device1.

**F.** Assign the Remote Help add-on license to User1.

**ANSWER: A B F**

**Explanation:**

Remote Help requires the Remote Help application to be installed on the managed Windows device that will participate in a session. Deploying the Remote Help app to Device1 through Intune ensures the device has the required client and can

receive Remote Help connections initiated from the Intune admin center. User1 must also receive appropriate Intune role-based access control permissions. The Help Desk Operator built-in role is suitable for support staff because it includes the Remote Help permissions needed to initiate remote assistance actions for devices within the user's assigned scope. Finally, Remote Help is separately licensed from the Microsoft 365 E5 base offering. Assigning the Remote Help add-on license to User1 provides the required entitlement for using the service; organizations can alternatively meet this entitlement through an applicable Intune Suite license assignment. Licensing must cover the users participating in Remote Help according to Microsoft's licensing requirements. Together, the deployed client, delegated Intune permissions, and assigned Remote Help entitlement allow User1 to use Remote Help for Device1. For implementation details, see Remote Help with Microsoft Intune and Role-based access control with Microsoft Intune.

## QUESTION NO: 20

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point,

**A.** From the Intune Company Portal, download Appl.

**B.** Create an OEMConfig profile.

**C.** From the Managed Google Play Store, approve App1.

**D.** Sync App1 with Intune.

## ANSWER: C D

**Explanation:**

For corporate-owned Android Enterprise fully managed devices, Intune uses Managed Google Play as the app source for public Android apps. **From the Managed Google Play Store, approve App1.** is required because approval authorizes the organization to make the selected Google Play app available through its Intune tenant. The administrator can locate the app in Managed Google Play from the Intune admin center and approve it for organizational use.

After approval, **Sync App1 with Intune.** imports the approved app's metadata into Intune. Once synchronization completes, the app is available in Intune's app list, where an administrator can configure assignments to the fully managed device group and select the appropriate installation intent, such as Required. This approval-and-sync workflow connects the Managed Google Play catalog to Intune and prepares the app for managed deployment at scale to the 500 enrolled devices. Microsoft documents the process of approving Managed Google Play apps and synchronizing them with Intune in its Add Managed Google Play apps to Android Enterprise devices with Intune guidance. For the Android Enterprise management model used here, see Set up Android Enterprise enrollment.

## QUESTION NO: 21

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

**A.** Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.

**B.** Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

**C.** Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.

**D.** Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

**ANSWER: B**

**Explanation:**

Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal is the required initial preparation step for Windows Autopilot when the devices have not already been registered by the OEM, distributor, or reseller. A device must be registered with the Windows Autopilot deployment service before it can be targeted with an Autopilot deployment profile and receive the intended out-of-box deployment experience.

For manually registering existing devices, the organization collects each device's Autopilot hardware hash (hardware ID) and creates a correctly formatted CSV file. The file is then imported into Intune, which registers the devices in the tenant. Following registration, administrators can assign the devices to the appropriate Microsoft Entra device group and apply an Autopilot deployment profile. This sequence ensures that, when a Phoenix office computer starts the Windows out-of-box experience, Autopilot can identify it as an organizational device and retrieve the assigned configuration. Microsoft documents manual registration as obtaining the hardware hash and importing the CSV file; the current management portal for this process is the Intune admin center. See Manually register devices with Windows Autopilot and Windows Autopilot registration overview.

## QUESTION NO: 22

You have a Microsoft 365 subscription that uses Microsoft Intune.

You create a Windows device configuration profile and assign the profile to the All devices group.

You need to ensure that the profile applies only to corporate-owned Windows devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create an assignment filter for devices with corporate ownership.

**B.** Apply the filter as an Include filtered devices in assignment filter.

**C.** Create a scope tag for corporate devices.

**D.** Create an app protection policy.

**E.** Apply the filter as an Exclude filtered devices in assignment filter.

**ANSWER: A B**

**Explanation:**

Create an **assignment filter** that evaluates the Windows device ownership property and includes corporate devices. Filters provide an additional targeting layer that evaluates device properties at assignment time.

You must then apply the filter as an **Include filtered devices in assignment** filter on the profile assignment. Because the profile is assigned to All devices, the include filter restricts the effective assignment to devices that match the corporate-ownership rule. A scope tag controls which administrators can view and manage Intune objects; it does not filter policy deployment. See Use filters when assigning apps, policies, and profiles in Microsoft Intune.

## QUESTION NO: 23

You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create an Azure AD group that has dynamic membership rules and uses the ZTDID tag.

**B.** Create an Azure AD group that has dynamic membership rules and uses the operatingSystem tag.

**C.** Assign a Windows Autopilot deployment profile to a group.

**D.** Join the computers to Azure AD.

**E.** Create a Group Policy object (GPO) that is linked to a domain.

**F.** Join the computers to an on-premises Active Directory domain.

**ANSWER: A C**

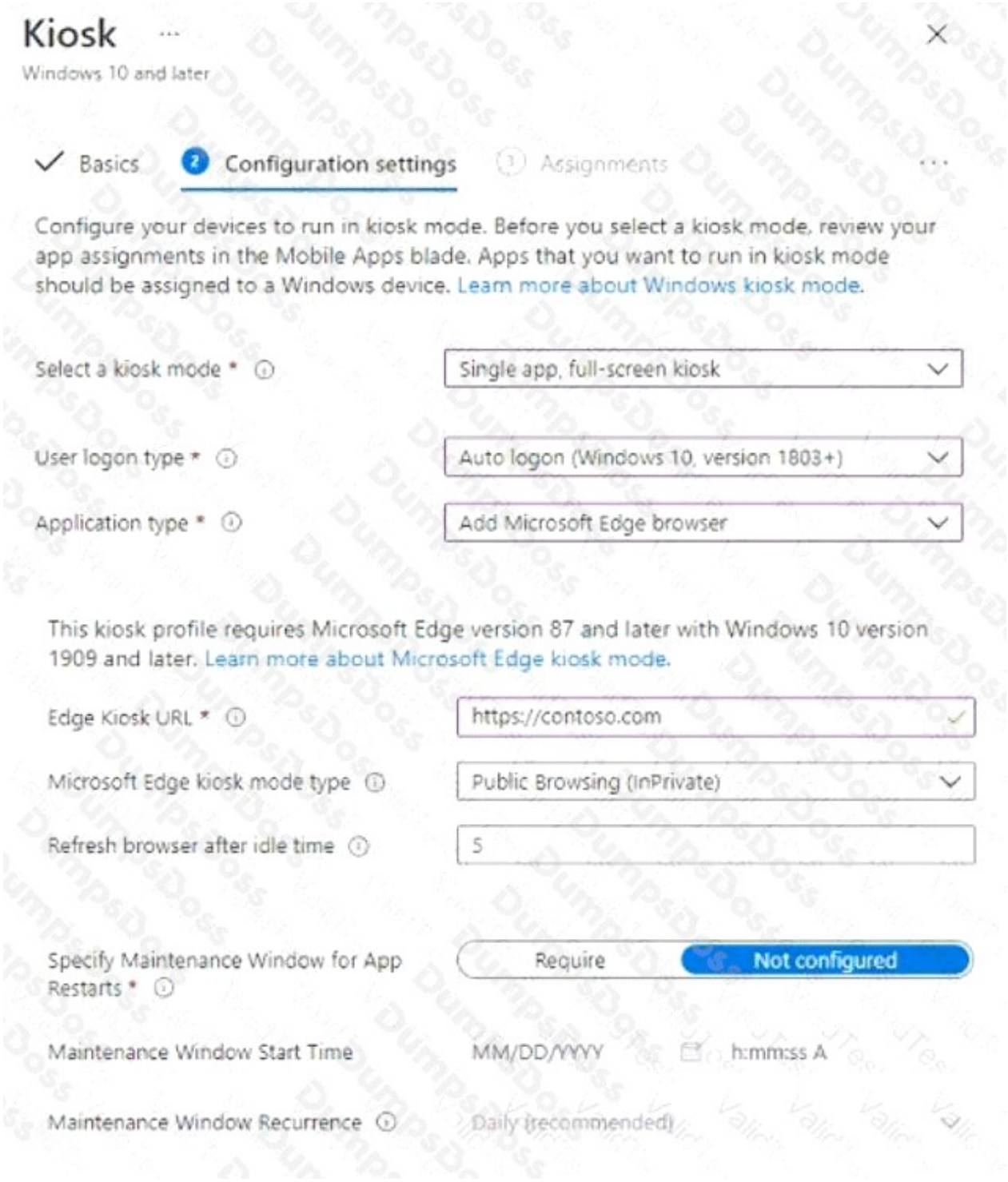
**Explanation:**

Create an Azure AD group that has dynamic membership rules and uses the ZTDID tag. This provides an automatically maintained device collection containing Windows Autopilot-registered devices. During Autopilot registration, a device receives a physical ID containing the `[ZTDId]` value. A dynamic device-membership rule that evaluates this physical ID, such as `device.devicePhysicalIDs -any (_ -contains "[ZTDId]")`, identifies Autopilot devices without requiring an administrator to manually add every current or future device to the group. This makes the assignment scalable and ensures newly registered Autopilot devices are included.

Assign a Windows Autopilot deployment profile to a group. Intune deployment profiles are assigned to Microsoft Entra device groups. Targeting the profile to the dynamic group means every device identified through the ZTDID-based rule receives the same Autopilot deployment settings when it goes through the Autopilot experience. Together, dynamic membership identifies the intended Autopilot device population, while the profile assignment applies the standardized configuration to that population. Microsoft documents the dynamic Autopilot device-group approach at Create an Autopilot device group and explains profile assignment in Windows Autopilot deployment profiles.

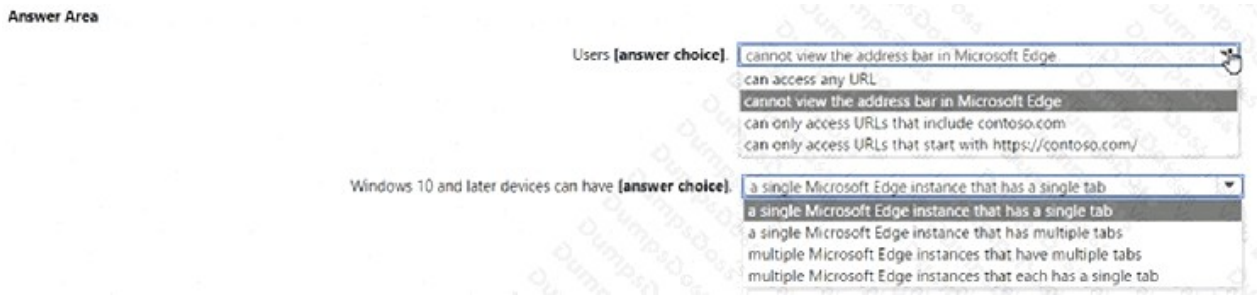
**QUESTION NO: 24 - (SIMULATION)**

You have the device configuration profile shown in the following exhibit.




Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

**Answer Area**




**ANSWER: See the explanation for the answer**

**Explanation:**

**Select:**

The profile is a **Single app, full-screen kiosk** using Microsoft Edge with the kiosk mode type set to **Public Browsing (InPrivate)**. The Edge Kiosk URL (`https://contoso.com`) is the initial/home URL; it is not an allowed-URL restriction. Public browsing supports browsing to other URLs and multiple tabs, but the single-app kiosk configuration limits the device to one Edge instance.

## QUESTION NO: 25

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

NOTE: Each correct selection is worth one point.

**A.** Privacy URL

**B.** Information URL

**C.** Developer

**D.** Owner

## ANSWER: A B

**Explanation:**

**Privacy URL** and **Information URL** are visible to users in Company Portal as part of the app's published details. These fields are configured on the App information page while adding or editing an Intune app. The Information URL supplies a user-facing link where employees can obtain additional details about the application, such as product documentation or support information. The Privacy URL provides a user-facing link to the app's privacy statement, allowing users to review how data related to the app may be handled before installing it.

Microsoft explicitly identifies both URLs as fields displayed in Company Portal. This helps make the self-service app catalog informative and transparent: users can review relevant product and privacy information directly from the catalog experience instead of needing to find those resources independently. The URLs are optional administrative metadata, but when configured, they are intended for Company Portal visibility. For the app-information field definitions and Company Portal behavior, see Add apps to Microsoft Intune. For Microsoft Store app deployment and configuration in Intune, see Add Microsoft Store apps to Microsoft Intune.

## QUESTION NO: 26

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

**A.** Microsoft Defender for Endpoint Power BI app

**B.** Microsoft Secure Score

**C.** Endpoint Analytics

**D.** Microsoft 365 Defender portal

**ANSWER: A**

**Explanation:**

Microsoft Defender for Endpoint Power BI app is designed to provide reporting and assessment views for Defender for Endpoint data, including security configuration assessment information. This assessment capability evaluates device security configurations against Microsoft-recommended baselines and presents the resulting configuration status in reportable, visual form. It enables an administrator to identify configuration gaps across managed Windows devices and investigate the settings that contribute to the assessment, making it appropriate when the requirement is specifically to compare the deployed Defender for Endpoint configuration with Microsoft's recommended baseline.

The app connects to Defender for Endpoint data through its APIs and provides prebuilt Power BI reports that can be used to examine the organization's security posture and configuration-related findings. This is especially useful where teams need an aggregated assessment across devices, rather than reviewing a single device's configuration individually. Microsoft documents the Power BI integration and available security reports at Microsoft Defender for Endpoint Power BI. For the underlying assessment concept and the way Defender for Endpoint monitors security configuration state, see Security configuration assessment.

## QUESTION NO: 27

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to deploy a custom root certificate to Windows devices and use the certificate to validate the certificate chain of an enterprise Wi-Fi server.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create a trusted certificate profile.

**B.** Associate the trusted certificate profile with the Wi-Fi profile.

**C.** Create a SCEP certificate profile only.

**D.** Create a PKCS certificate profile only.

**E.** Create an app configuration policy.

**ANSWER: A B**

**Explanation:**

**Create a trusted certificate profile** is required to deploy the root certification authority certificate to the Windows devices. A trusted certificate profile places the certificate in the appropriate trusted certificate store so that Windows can validate certificates issued by that authority.

**Associate the trusted certificate profile with the Wi-Fi profile** configures the Wi-Fi connection to use the deployed trusted root certificate when validating the server certificate during authentication. This helps protect users from connecting to an untrusted wireless authentication server.

A SCEP certificate profile issues an identity certificate to a user or device and is not required merely to deploy a trusted root. A PKCS certificate profile also issues identity certificates. An app configuration policy does not manage Wi-Fi certificate trust. For more information, see Configure certificates with Microsoft Intune and Add Wi-Fi settings for Windows devices in Intune.

## QUESTION NO: 28 - (HOTSPOT)

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to review and implement Microsoft 365 Defender device onboarding. The solution must meet the following requirements:

• View onboarded devices that have the Chromium-based version for Microsoft Edge installed.

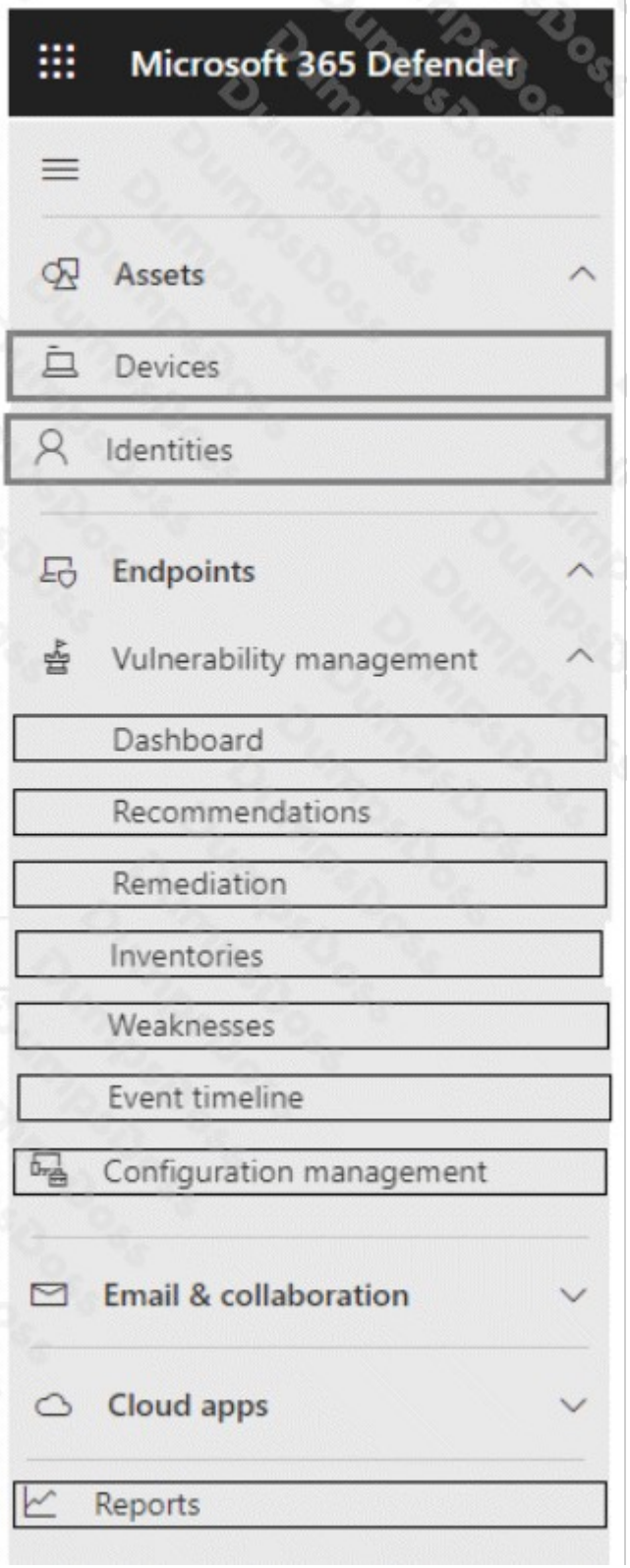
• Download an onboarding package for a Windows 11 device.

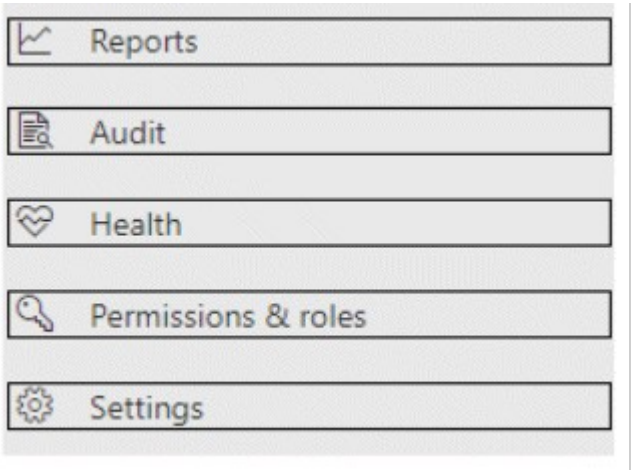
• Minimize administrative effort.

Which two settings should you use in the Microsoft 365 Defender portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

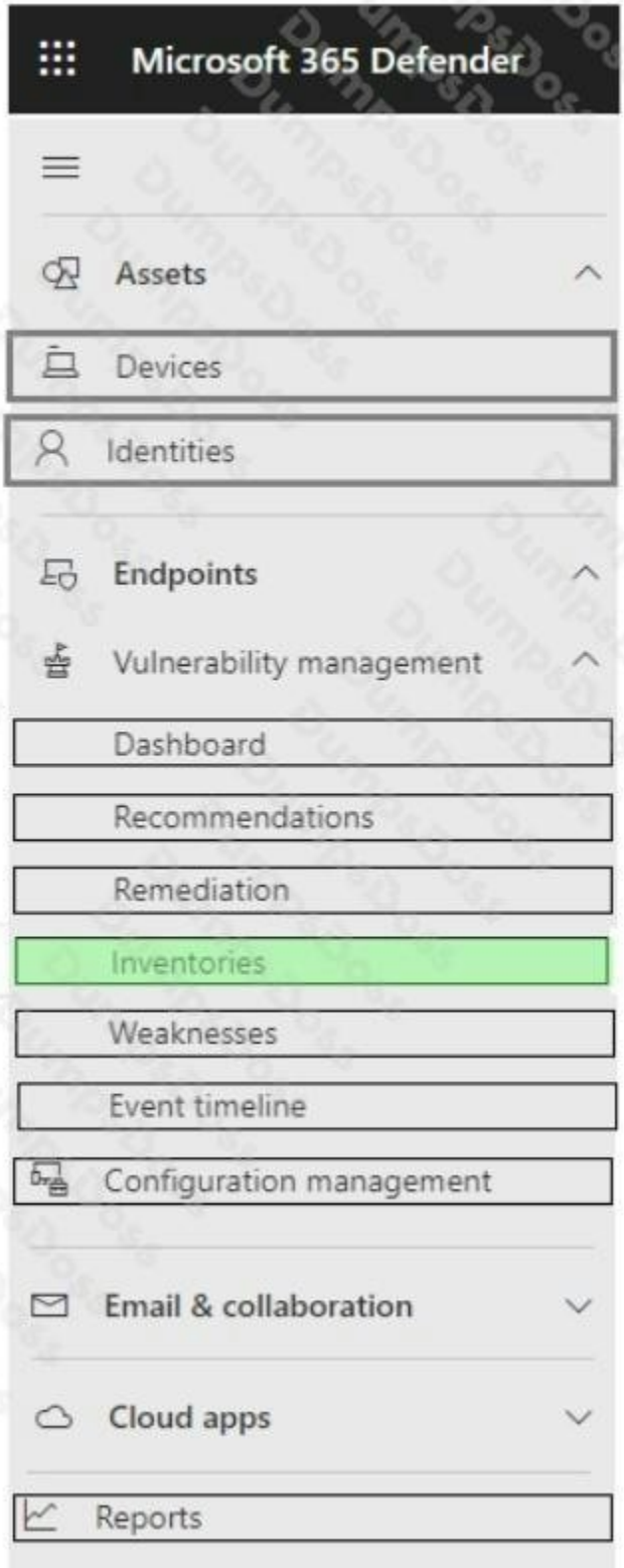
## Answer Area


Microsoft 365 Defender
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Configuration management
Email & collaboration
Cloud apps
Reports




**ANSWER:**

## Answer Area


Microsoft 365 Defender
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Configuration management
Email & collaboration
Cloud apps
Reports

**Explanation:**

**Inventories** is the appropriate setting for identifying onboarded devices that have the Chromium-based Microsoft Edge installed. In Microsoft Defender Vulnerability Management, Software inventory provides a centralized view of software discovered across managed and onboarded endpoints. An administrator can search the inventory for Microsoft Edge, open its software details, and view the devices on which that software is present. This provides the requested device visibility directly in the Defender portal and avoids checking individual device records or collecting software information manually. The inventory experience is designed to correlate installed software with device information, which makes it the practical choice when the goal is to locate devices running a particular application. Microsoft documents this capability in Software inventory in Microsoft Defender Vulnerability Management.

**Settings** is the appropriate setting for obtaining the Windows 11 onboarding package. In the Microsoft 365 Defender portal, Defender for Endpoint onboarding is accessed from **Settings**, then **Endpoints**, followed by **Device management** and **Onboarding**. The onboarding page lets an administrator choose the Windows client operating system and deployment method, then download the onboarding package or script needed to enroll the device in Defender for Endpoint. Using this built-in portal workflow minimizes administrative effort because it supplies the supported onboarding artifacts without requiring a custom configuration or a separate management interface. Microsoft's onboarding guidance, including the portal-based onboarding workflow for Windows devices, is available at Onboard devices to Microsoft Defender for Endpoint.

## QUESTION NO: 29

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have 100 Windows 11 devices enrolled in Intune.

You need to configure Microsoft Defender Antivirus to perform a daily quick scan and to prevent users from excluding files or folders from scans.

Which two settings should you configure in an Endpoint security antivirus policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Configure the scheduled scan type as Quick scan.

**B.** Set Allow users to exclude files and folders from scans to No.

**C.** Enable network protection.

**D.** Enable controlled folder access.

**E.** Create a firewall policy.

## ANSWER: A B

**Explanation:**

**Configure the scheduled scan type as Quick scan** configures Microsoft Defender Antivirus to run a quick scan during the scheduled scan. The daily schedule can be defined through the scheduled scan settings in the antivirus policy.

**Set Allow users to exclude files and folders from scans to No** prevents local users from adding file and folder exclusions. This reduces the risk that a user can exempt malicious content from Microsoft Defender Antivirus scanning.

Network protection and controlled folder access are separate security features and do not configure scheduled scan type or user-controlled antivirus exclusions. A firewall policy manages network filtering rather than antivirus scan behavior. For more information, see Microsoft Defender Antivirus policy settings in Intune.

## QUESTION NO: 30

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** From the Intune Company Portal, download App1.

**B.** Sync App1 with Intune.

**C.** From the Managed Google Play Store, approve App1.

**D.** Create an OEMConfig profile.

## ANSWER: B C

**Explanation:**

For Android Enterprise fully managed devices, public Android applications are acquired and managed through the managed Google Play integration in Microsoft Intune. The required preparation workflow begins with **From the Managed Google Play Store, approve App1.** Approval adds the public application to the organization's managed Google Play app collection and authorizes the organization to use it for managed Android Enterprise deployments. This is performed in the managed Google Play pane opened from Intune when adding a managed Google Play app.

After approval, **Sync App1 with Intune.** Synchronization imports the approved app's metadata into the Intune admin center, where it becomes an Intune app object. The administrator can then configure assignments, such as making the app required for groups containing the corporate-owned fully managed devices. This two-step approval-and-sync process is the supported approach for making public managed Google Play apps available for deployment to Android Enterprise devices. Microsoft documents the approval and synchronization process in its guidance for adding managed Google Play apps to Android Enterprise devices; assignment is then performed using Intune's app assignment workflow.

## QUESTION NO: 31

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

• Install Windows 11 Enterprise on each device.

• Install a Windows Installer (MSI) package named App1 on each device.

• Add a certificate named Certificate1 that is required by App1.

• Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** subscription activation

**B.** a custom Windows image

**C.** an in-place upgrade

**D.** Windows Autopilot

**E.** provisioning packages

**ANSWER: B D E**

**Explanation:**

**a custom Windows image**, **Windows Autopilot**, and **provisioning packages** can each provide an end-to-end provisioning approach for these devices. A custom Windows image can be based on Windows 11 Enterprise and prepared with required software and certificates before deployment. The deployment process can then take the device through Windows setup and organizational identity configuration, including Microsoft Entra ID (formerly Azure AD) join.

**Windows Autopilot** supports provisioning new Windows devices through the out-of-box experience. An Autopilot deployment profile can join devices to Microsoft Entra ID and enroll them in Intune. Intune can deploy App1 as a required Windows app, deliver Certificate1 through a certificate profile, and apply the Enterprise edition entitlement for eligible licensed users. This provides cloud-managed setup without maintaining a traditional device image. See Windows Autopilot overview.

**provisioning packages**, created with Windows Configuration Designer, can apply configuration during setup without conventional reimaging. A package can contain an edition-upgrade configuration, application-installation commands for an MSI, certificate payloads, and organizational settings for Microsoft Entra ID join. This makes the package a suitable repeatable provisioning mechanism for a small set of new devices. Microsoft documents the supported package capabilities and deployment model at Provisioning packages for Windows.

## QUESTION NO: 32

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You have a device named Devic1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Deploy the Remote Help app to Device1.

**B.** Assign the Help Desk Operator role to User1.

**C.** Assign the Intune Administrator role to User1.

**D.** Assign a Microsoft 365 E5 license to User1.

**E.** Rerun device onboarding on Device1.

**F.** Assign the Remote Help add-on license to User1.

**ANSWER: A B F**

**Explanation:**

Remote Help requires preparation of both the managed device and the user who will provide assistance. Deploying the Remote Help app to Device1 makes the Remote Help client available on the enrolled Windows device, which is necessary for a Remote Help session to be established. The application can be deployed through Intune as a Windows app, enabling the managed device to receive and run the Remote Help client.

Assigning the Help Desk Operator role to User1 provides the required Intune role-based access control permissions for remote assistance. This built-in Intune role includes Remote Help permissions that allow a helper to view a user's screen and take full control, provided the role assignment scope includes Device1.

Assigning the Remote Help add-on license to User1 provides the licensing entitlement for the helper to use Remote Help. Microsoft requires Remote Help licensing for both the helper and the user receiving assistance. An Intune Suite entitlement can also satisfy this requirement; however, assigning the Remote Help add-on is a valid way to provide the needed Remote Help license. Microsoft 365 E5 alone does not grant the Remote Help entitlement. For licensing, deployment, and RBAC requirements, see Remote Help with Microsoft Intune and Use Remote Help on Windows devices.

## QUESTION NO: 33

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11.

You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

• For the WinRM service, set Startup type to Automatic.

• Create a listener that accepts requests from any IP address.

• Enable a firewall exception for WS-Management communications.

Which PowerShell cmdlet should you use?

**A.** Connect-WSMan

**B.** Enable-PSRemoting

**C.** Invoke-WSManAction

**D.** Enable-PSSessionConfiguration

## ANSWER: B

**Explanation:**

**Enable-PSRemoting** performs the standard local configuration needed for a Windows device to receive PowerShell remoting connections through Windows Remote Management (WinRM). When it is run in an elevated PowerShell session, the cmdlet configures WinRM for remoting by starting the WinRM service and setting its startup type to Automatic. This ensures the service is available after future device restarts without requiring a manual start.

The cmdlet also invokes the required WS-Management quick-configuration tasks. These tasks create the WinRM listener that accepts requests on the device's network addresses and enable the applicable Windows Defender Firewall rules for WS-Management traffic. The default WinRM HTTP listener uses TCP port 5985, allowing appropriately authorized remote-management clients to establish PowerShell remoting sessions. In an Active Directory domain, the firewall rules are enabled for the appropriate domain network profile, which supports the stated domain-based scenario.

This cmdlet is the supported PowerShell method for preparing a Windows 11 computer to accept incoming remote PowerShell commands while applying the requested service, listener, and firewall settings. Microsoft documents the configuration actions performed by Enable-PSRemoting and describes the underlying WS-Management setup in Installation and configuration for Windows Remote Management.

## QUESTION NO: 34

You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create a device configuration profile.

**B.** Enroll the devices in Microsoft Intune by using the Intune Company Portal.

**C.** Create a compliance policy.

**D.** Create an iOS app provisioning profile.

**E.** Enroll the devices in Microsoft Intune by using Apple Business Manager.

**ANSWER: A E**

**Explanation:**

**Create a device configuration profile.** is required because Intune applies iOS/iPadOS software-update management settings through device configuration. For supervised Apple devices, an update policy can target a chosen operating-system version and schedule its download and installation. The policy can also control the availability of newer updates, including using Apple software-update deferral controls where appropriate, so users do not install an unapproved release before the organization permits it. This management is device-based and requires the iPad to be under Intune management with the applicable supervision capabilities.

**Enroll the devices in Microsoft Intune by using Apple Business Manager.** provides Automated Device Enrollment for organization-owned iPads. Automated Device Enrollment places the devices under supervised management during setup, which is necessary for the enhanced iOS/iPadOS software-update controls used to manage, schedule, and restrict operating-system updates. With the devices assigned to the Intune MDM server in Apple Business Manager and enrolled through this method, Intune can reliably apply the configuration/update policy at scale to all 100 devices. Microsoft documents the supervised enrollment process and the software-update policy requirements at Automatically enroll iOS/iPadOS devices with Apple Business Manager and Manage iOS/iPadOS software updates in Intune.

**QUESTION NO: 35**

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You add apps to Intune as shown in the following table.

| Name | App type |
|---|---|
| App1 | Android store app |
| App2 | Android line-of-business app |
| App3 | Managed Google Play store app |

You need to create an app configuration policy named Policy1 for the Android Enterprise platform.

Which apps can you manage by using Policyl1?

**A.** App2 only

**B.** App3 only

**C.** App1 and App3 only

**D.** App2 and App3 only

**E.** App1, App2, and App3

**ANSWER: D**

**Explanation:**

**App2 and App3 only** is correct because an Android Enterprise app configuration policy in Intune can deliver configuration settings to supported Managed Google Play apps and Android line-of-business apps. These policies provide app-specific settings before or after deployment, allowing an organization to configure an app consistently for targeted users or devices. Settings are delivered through the Android Enterprise management channel and must be supported by the app developer; for example, an app can expose managed configuration keys that Intune sends as part of the policy. Intune supports app configuration policies for Android Enterprise in managed-device scenarios, and it supports configuring both Managed Google Play and line-of-business apps where the application supports managed app configuration. Therefore, Policy1 can manage the apps represented by App2 and App3 in the table. For implementation details, including the requirements for Android Enterprise managed devices and Managed Google Play app configuration, see App configuration policies for Android Enterprise. Microsoft also documents the supported app types and configuration-policy behavior in its app configuration policies overview.

**QUESTION NO: 36**

You have a Microsoft 365 tenant that contains the objects shown in the following table.

| Name | Type |
|---|---|
| Admin1 | User |
| Group1 | Microsoft 365 group |
| Group2 | Distribution group |
| Group3 | Mail-enabled security group |
| Group4 | Security group |

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

**A.** Group3 and Group4 only

**B.** Admin1, Group3, and Group4 only

**C.** Group1, Group3, and Group4 only

**D.** Group1, Group2, Group3, and Group4 only

**E.** Admin1, Group1. Group2, Group3, andGroup4

**ANSWER: C**

**Explanation:**

**Group1, Group3, and Group4 only** is correct. Microsoft Intune app assignments are made to Microsoft Entra groups rather than directly to an individual administrative user account. For a Microsoft 365 Apps suite deployment, Intune supports assigning the app to eligible user groups and device groups. This lets an administrator deploy the Office apps according to either the people who require the software or the managed devices on which it must be installed.

The groups represented by Group1, Group3, and Group4 are eligible assignment targets for App1 based on their group characteristics shown in the table. When configuring the app's *Assignments* pane, these groups can be selected and configured with an appropriate intent, such as Required or Available for enrolled devices where supported. Intune then evaluates group membership and applies the Microsoft 365 Apps deployment to the applicable users or devices.

Using group-based assignment is also the supported operational model for scalable app deployment and lifecycle management. Membership changes are evaluated by Microsoft Entra ID and Intune, so devices and users receive the

intended app deployment as they enter the assigned groups. For details, see Microsoft 365 Apps deployment in Intune and Add and assign apps in Intune.

## QUESTION NO: 37

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

**A.** failure events from the Security log

**B.** the list of processes and their execution times

**C.** the average processor utilization

**D.** error events from the System log

**E.** third-party application logs stored as text files

## ANSWER: C D E

**Explanation:**

The average processor utilization can be collected by configuring Windows performance counters for the Log Analytics workspace. Performance-counter collection records sampled counter values from managed Windows devices, including processor counters such as `\Processor(_Total)\% Processor Time`. This enables administrators to query, aggregate, and trend CPU utilization across the endpoint fleet.

Error events from the System log can be collected through Windows event-log collection. The Log Analytics agent can send selected Windows event records to the workspace, and collection can be scoped to a specific log and severity level. System-log errors are therefore available for centralized investigation and correlation with other monitoring data.

Third-party application logs stored as text files can be collected as custom text logs. After defining the file path and a timestamp format that identifies individual records, Log Analytics ingests the entries into a custom log table. This supports centralized search and analysis of application-generated text logs alongside event and performance data. Microsoft documents these supported agent data sources, including performance counters, Windows event logs, and custom logs, in Log Analytics agent data sources. For custom text-log configuration requirements, see Collect custom text logs with the Log Analytics agent.

## QUESTION NO: 38

You have a Microsoft 365 subscription that contains a user named User1 and 500 Windows devices enrolled in Microsoft Intune.

You configure an attack surface reduction {ASR) rule and enable the rule in Warn mode.

User1 downloads a file named file1.exe. When User1 attempts to run file1.exe he receives a prompt that the content has been blocked. The user unblocks the content.

How much time will pass until the user is prompted next to unblock the content?

**A.** 10 minutes

**B.** one hour

**C.** 24 hours

**D.** one week

## ANSWER: C

**Explanation:**

**24 hours** is correct. When an attack surface reduction rule is configured in warn mode, Windows displays a warning when activity triggers that rule and gives the user the opportunity to bypass the warning. If the user selects the option to unblock or allow the activity, the bypass is temporary. Microsoft specifies that the user can continue performing that specific action without another warning for 24 hours. After the 24-hour bypass period expires, the ASR rule is enforced again for the activity, and the user will be shown the warning prompt if they attempt the action again. This behavior enables organizations to deploy ASR protections while monitoring impact and permitting limited, time-bound user overrides where appropriate. The temporary bypass applies to the warned activity and does not permanently disable the ASR rule or change the device's assigned Intune policy. Administrators can use Microsoft Defender reporting and security telemetry to evaluate warn-mode events before deciding whether to move the rule to block mode. See Microsoft's ASR rules deployment guidance and the ASR rules reference.

## QUESTION NO: 39

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage all Windows 11 devices.

You create an attack surface reduction (ASR) policy named Profile1 based on the Attack Surface Reduction Rules profile and assign Profile! to all the devices.

A user reports that an Adobe Reader plug-in is now blocked.

You need to ensure that the plug-in is unblocked.

What should you do?

**A.** Create an Endpoint Privilege Management policy and assign the policy to all the devices.

**B.** Add a scope tag to Profile1.

**C.** Configure ASR Only Per Rule Exclusions in Profile1.

**D.** Create a device compliance policy and assign the policy to all the devices.

## ANSWER: C

**Explanation:**

Configure ASR Only Per Rule Exclusions in Profile1. Attack surface reduction rules can block behavior associated with a legitimate application or plug-in when that behavior matches the protection criteria of an enabled rule. Intune supports exclusions scoped to an individual ASR rule, allowing the administrator to exempt the specific Adobe Reader plug-in file, folder path, or process from the rule that is generating the block while keeping other ASR protections enabled. This is the appropriate least-privilege approach because the exception is limited to the affected rule and application component rather than reducing protection broadly across the device estate. Before adding the exclusion, identify the exact ASR rule and the precise process, file, or path reported in Defender or Intune event data. Then add that value under the per-rule exclusions setting for the relevant ASR rule in the existing Attack Surface Reduction Rules profile and deploy the updated profile to the targeted devices. Microsoft documents that ASR-only per-rule exclusions apply only to the selected rule and are intended for situations where a specific ASR rule must allow a known, trusted item. See Microsoft Intune attack surface reduction policy settings and Microsoft Defender ASR rules deployment guidance.

## QUESTION NO: 40

You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

**A.** the Azure portal app

**B.** Endpoint analytics

**C.** the Company Portal app

**D.** Microsoft Power BI

**ANSWER: D**

**Explanation:**

Microsoft Power BI is the appropriate tool for creating a custom device inventory report from Intune Data Warehouse data. The Intune Data Warehouse provides historical Intune data through an OData feed, including device, user, application, compliance, and configuration-related entities. Power BI Desktop can connect to that OData feed, load the available warehouse entities into a data model, and create tailored visuals, filters, calculations, and dashboards that meet inventory-reporting requirements.

In the Intune admin center, an administrator can retrieve the Data Warehouse feed link and use Power BI's OData connector to authenticate and import the data. The resulting report can be refined to show the inventory information needed, such as device details, ownership, operating-system information, enrollment data, and other fields available in the warehouse. This approach is designed for custom analytics and reporting based on the Data Warehouse dataset, including reports that go beyond the standard views in the Intune admin center.

Microsoft documents the Data Warehouse-to-Power-BI workflow in Create reports using the Intune Data Warehouse and explains how to obtain the feed URL in Get a Power BI link to the Intune Data Warehouse.

## QUESTION NO: 41

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace. Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.

NOTE: Each correct selection is worth one point.

**A.** error events from the System log

**B.** failure events from the Security log

**C.** third-party application logs stored as text files

**D.** the list of processes and their execution times

**E.** the average processor utilization

**ANSWER: A C E**

**Explanation:**

The supported data types are **error events from the System log**, **third-party application logs stored as text files**, and **the average processor utilization**. Azure Monitor Logs can ingest Windows Event Log records from client devices, including events from the System channel. A data collection rule can filter event collection by event level, so error-level System events can be sent to the Log Analytics workspace and queried in the Event table.

Text-based logs produced by third-party applications can be collected as custom text logs. Azure Monitor can monitor specified file paths and send new records from those files to a Log Analytics workspace, where the records become available for Kusto Query Language analysis and alerting.

Processor utilization is collected through Windows performance counters. A collection rule can gather counters such as *Processor Information\% Processor Time*; once stored in the Perf table, a query can calculate an average utilization value for a computer or group of computers over a selected time range. These collection mechanisms enable centralized operational monitoring of Windows endpoints. For implementation details, see Collect performance data with the Azure Monitor Agent and Collect text logs with the Azure Monitor Agent.

## QUESTION NO: 42

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

**A.** a device restrictions device configuration profile

**B.** an app configuration policy

**C.** a Windows 10 and later security baseline

**D.** a custom device configuration profile

**E.** a Windows 10 and later update ring

**ANSWER: D E**

**Explanation:**

A custom device configuration profile can prevent Windows Insider enrollment by configuring the Windows Policy CSP setting **System/AllowBuildPreview** through a custom OMA-URI. This policy controls whether users can access and manage Windows Insider Preview build settings. Setting it to disallow preview builds removes the user's ability to use the Windows Settings experience to enroll the device in the Windows Insider Program. This is an appropriate approach when the organization needs direct control of a specific Windows policy setting through Intune. Microsoft documents the policy and its supported configuration through the Policy CSP - System documentation.

A Windows 10 and later update ring is also a complete solution because update rings expose Windows Update for Business servicing controls, including the setting for managing Windows Insider or pre-release builds. Configuring the pre-release-build behavior to disable or block Insider builds centrally applies the organization's servicing policy to assigned Windows devices, rather than allowing users to select an Insider channel themselves. Update rings are specifically intended to manage Windows update behavior and are deployed to device groups in Intune. For the available Windows Update settings and their use in Intune, see Windows update settings for Intune.

**QUESTION NO: 43**

You have a Microsoft 365 subscription.

Each user is assigned a Windows 365 Enterprise license.

You need to deploy Cloud PCs that will be Microsoft Entra hybrid joined.

What should you do first?

**A.** Create an Azure network connection (ANC).

**B.** Create a provisioning policy.

**C.** Create a configuration profile in Microsoft Intune.

**D.** Upload a custom image.

**ANSWER: A**

**Explanation:**

Create an Azure network connection (ANC) first. Microsoft Entra hybrid joined Cloud PCs must be provisioned into an Azure virtual network that has connectivity to the organization's on-premises Active Directory Domain Services environment. The ANC supplies Windows 365 with the required Azure virtual network and subnet, DNS server settings, and Active Directory domain-join configuration. It is therefore the foundational networking resource for this deployment model.

After the ANC is created, Windows 365 performs health checks to validate essential prerequisites, including communication with the domain, DNS resolution, the necessary service endpoints, and the permissions used to join devices to the domain. A healthy ANC can then be selected when a provisioning policy is configured for Microsoft Entra hybrid join. This sequence ensures that Cloud PC provisioning has a validated network path and domain-join capability before devices are assigned to users.

Microsoft documents that Azure network connections enable Cloud PCs to communicate with on-premises resources and are required for Microsoft Entra hybrid join scenarios. For implementation details, see Azure network connections overview and Create an Azure network connection.

## QUESTION NO: 44

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following

requirements:

• Ensure that you can manage the personal devices by using Microsoft Intune.

• Ensure that users can access company data seamlessly from their personal devices.

• Ensure that users can only sign in to their personal devices by using their personal account.

What should you use to add the devices to Azure AD?

**A.** Azure AD registered

**B.** hybrid Azure AD join

**C.** Azure AD joined

## ANSWER: A

**Explanation:**

Azure AD registered is the appropriate device identity state for personally owned, bring-your-own-device Windows 11 devices. With registration, the user continues to sign in to Windows by using their personal local account or personal Microsoft account. They then add their work or school account to connect the device to the organization. This preserves the required personal sign-in experience while establishing a Microsoft Entra ID (formerly Azure AD) device record associated with the user and organization.

That connection enables seamless access to company resources through the user's work identity, including single sign-on where supported, while allowing the device to be enrolled in Microsoft Intune for MDM. Intune enrollment can be initiated from Windows Settings when the user connects a work or school account, subject to the organization's enrollment and compliance policies. This model is specifically intended for personal devices that need access to organizational data and management without changing the Windows sign-in identity to an organizational account.

Microsoft identifies Microsoft Entra registered devices as personally owned devices that are signed in with a local or Microsoft account and connected to work resources. See What is a device identity? and Enroll a Windows device in Intune.

## QUESTION NO: 45

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

**A.** an app configuration policy

**B.** a security baseline

**C.** an app protection policy

**D.** an iOS app provisioning profile

**ANSWER: C**

**Explanation:**

**an app protection policy** is the correct configuration because Intune app protection policies (also called mobile application management, or MAM, policies) govern how organizational data is handled within supported managed apps on iOS and iPadOS. This approach protects corporate data at the application layer, so it can be applied to managed apps regardless of whether a device is enrolled in Intune.

When creating an iOS/iPadOS app protection policy, configure the data-protection setting named **Printing org data** and set it to **Block**. This prevents users from printing organization data from the apps targeted by the policy. The policy can be assigned to the users who access corporate information through apps such as Microsoft Outlook, Microsoft Teams, and Microsoft 365 apps, ensuring that the restriction follows the user and protected app data.

Microsoft documents printing as a data-transfer control in Intune app protection policies for iOS/iPadOS. For implementation details and the available data-protection settings, see App protection policy settings for iOS/iPadOS. For an overview of how app protection policies protect organizational data in managed apps, see App protection policies overview.

## QUESTION NO: 46

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled.

From Computer1, you connect to Computer2 by using Remote Desktop Connection.

You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.

What should you do?

**A.** From Computer2, configure the Remote Desktop settings.

**B.** From Windows Defender Firewall on Computer1, allow Remote Desktop.

**C.** From Windows Defender Firewall on Computer2, allow File and Printer Sharing.

**D.** From Computer1, configure the Remote Desktop Connection settings.

**ANSWER: D**

**Explanation:**

From Computer1, configure the Remote Desktop Connection settings. Local-drive access during a Remote Desktop session is enabled through device and resource redirection in the Remote Desktop Connection client on the computer that initiates the connection. Before connecting, open Remote Desktop Connection, select **Show Options**, go to **Local Resources**, and select **More** in the Local devices and resources section. You can then select the drives on Computer1 that must be available in the session. After the connection is established, the redirected drives are displayed in File Explorer on Computer2 within the remote session, commonly under **This PC**, and can be used to open, save, and copy files.

This is a client-connection setting: Computer1 is the Remote Desktop client and is therefore where the selection of local resources to redirect is made. The remote host accepts the Remote Desktop connection, while the client determines which of its locally attached devices and drives it offers to the remote session. Microsoft documents Remote Desktop resource redirection, including access to local drives, in its Remote Desktop client guidance. See Allow access to local resources in a Remote Desktop session and Remote Desktop clients.

## QUESTION NO: 47

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have the devices shown in the following table.

| Name | Operating system | Activation type |
|---|---|---|
| Device1 | Windows 10 Pro for Workstation | Key |
| Device2 | Windows 11 Pro | Key |
| Device3 | Windows 11 Pro | Subscription |

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

**A.** Device3 only

**B.** Device2 and Device3 only

**C.** Device1 and Device2 only

**D.** Device1, Device2, and Device3

**ANSWER: B**

**Explanation:**

**Device2 and Device3 only** is correct. Windows subscription activation performs an edition step-up when an eligible, licensed user signs in to a supported device. For Windows 11 Enterprise, the device must already run Windows 11 Pro and meet the required Microsoft Entra device-identity condition, such as being Microsoft Entra joined or hybrid Microsoft Entra joined. The signing-in user must also be assigned an eligible Windows Enterprise subscription license, for example a license included with an appropriate Microsoft 365 Enterprise plan.

Subscription activation is specifically an edition activation capability: it unlocks Enterprise features on the installed matching Windows version without requiring a product key or a reimage. It does not perform an in-place operating-system upgrade from Windows 10 to Windows 11. Device2 and Device3 satisfy the required Windows 11 Pro, identity, and licensing conditions shown in the table, so they can automatically transition to Windows 11 Enterprise when the eligible licensed user signs in. Microsoft documents the supported editions, join states, and licensing prerequisites in its Windows subscription activation documentation and describes how Intune can manage edition upgrades in the Windows edition upgrade policy documentation.

**QUESTION NO: 48**

You have a Microsoft 365 tenant that contains the devices shown in the following table.

| Name | Member of |
|---|---|
| Device1 | Group1 |
| Device2 | Group1 |
| Device3 | Group1 |

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the

device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not

compliant.

What should you do from the Microsoft Intune admin center?

**A.** From Device compliance, configure the Compliance policy settings.

**B.** From Endpoint security, configure the Conditional access settings.

**C.** From Tenant administration, modify the Diagnostic settings.

**D.** From Policy1, modify the actions for noncompliance.

**ANSWER: A**

**Explanation:**

From Device compliance, configure the Compliance policy settings. Intune includes a tenant-wide compliance setting named **Mark devices with no compliance policy assigned as**. This setting determines the compliance state assigned to enrolled devices that are not targeted by any device compliance policy. The described behavior occurs when this tenant-level setting permits devices with no assigned compliance policy to be reported as compliant.

Configure **Mark devices with no compliance policy assigned as** to **Not compliant**. Intune will then report a device as compliant only when the device receives a compliance policy and successfully meets that policy's requirements. Devices outside the assignment scope of all compliance policies, including devices that are not members of Group1 when Policy1 is the only applicable policy, will be evaluated as not compliant. This is a global compliance-evaluation behavior and is configured separately from settings within an individual compliance policy.

Microsoft documents this setting in its guidance for device compliance policies in Intune. The Intune settings catalog reference also describes the tenant-level compliance policy settings at Create a compliance policy for Windows devices.

## QUESTION NO: 49

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Intune to manage all devise.

Users have iOS devices with Microsoft apps installed.

You need to prevent users from cutting, copying, and pasting data between Microsoft Excel and other apps installed on the devices.

What should you configure?

**A.** an app protection policy

**B.** an app configuration policy

**C.** an iOS app provisioning profile

**D.** policies for Microsoft Office apps

**ANSWER: A**

**Explanation:**

An app protection policy is the appropriate Intune control because it applies data-protection rules directly to supported Microsoft apps, including Microsoft Excel on iOS and iPadOS. In an iOS/iPadOS app protection policy, the Data protection settings include the *Restrict cut, copy, and paste between other apps* control. An administrator can configure this setting to block clipboard transfers entirely or to limit transfers so that organizational data remains within policy-managed applications. This protects work or school content handled by Excel from being copied into unmanaged apps on the device.

App protection policies are part of Intune mobile application management and are designed to protect organizational data at the application layer. They can be used with enrolled devices and, where supported, without requiring device enrollment. The policy must be targeted to the appropriate users and include Excel among its protected apps so that the clipboard restriction is enforced when users work with organizational data in Excel. Microsoft describes app protection policies and their data-transfer controls in its Intune app protection policy documentation and the iOS/iPadOS app protection policy settings reference.

## QUESTION NO: 50 - (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 |
| User1 | None |

You purchase the devices shown in the following table.

| Name | Operating system |
|---|---|
| Device1 | Windows 11 |
| Device2 | Android |

Administrators perform the following actions:

• Join Device1 to contoso.com by using the credentials of Admin1.

• Register Device2 in contoso.com by using the credentials of Admin2.

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 Admin2 credentials can be used to sign in to Device1. | ○ | ○ |
| The Admin2 credentials can be used to sign in to Device2. | ○ | ○ |
| The credentials of User1 can be used to sign in to Device1. | ○ | ○ |

**ANSWER:**

**Explanation:**

Device1 is running Windows 11 and is joined to contoso.com, which means it is a Microsoft Entra joined Windows device. Microsoft Entra joined devices use Microsoft Entra identities for Windows sign-in. Consequently, Admin2 can sign in to Device1 using the Admin2 contoso.com credentials. Admin2 also has the Cloud Device Administrator role. This role provides local administrator rights on Microsoft Entra joined devices, which supports administration of Device1 after sign-in. User1 is also a user in the same Microsoft Entra tenant. A standard tenant user can sign in to a Microsoft Entra joined Windows device unless a policy has been configured to restrict sign-in, and no such policy is described. Therefore, User1 can sign in to Device1 as well.

Device2 is different because it runs Android and was registered rather than joined. Microsoft Entra registration on an Android device creates a workplace association between the device and the organization, generally to enable access to organizational resources and management scenarios. It does not turn an Android device's operating-system sign-in into a Microsoft Entra Windows-style sign-in experience. Thus, Admin2's credentials cannot be used to sign in to Device2 in the sense stated. The correct selections are Yes for Admin2 signing in to Device1, No for Admin2 signing in to Device2, and Yes for User1 signing in to Device1. Microsoft documents the distinction between registered and joined devices at What is a device identity?, and documents the Cloud Device Administrator role at Microsoft Entra built-in roles.

## QUESTION NO: 51

You have a Microsoft Intune subscription.

You have devices enrolled in intune as shown in the following table.

| Name | Operating system |
|---|---|
| Device1 | Android 8.1.0 |
| Device2 | Android 9 |
| Device3 | iOS 11.4.1 |
| Device4 | iOS 12.3.1 |
| Device5 | iOS 12.3.2 |

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage Appl ?

**A.** 1

**B.** 2

**C.** 3

**D.** 4

**E.** 5

**ANSWER: B**

**Explanation:**

2 is the minimum number of app configuration policies because App1 is installed on enrolled devices that use two distinct mobile platforms: iOS/iPadOS and Android. For enrolled devices, Intune uses app configuration policies for managed devices. These policies deliver application settings through the Intune device-management channel and are created for a specific platform. Consequently, the settings for App1 must be defined in one policy targeting the iOS/iPadOS devices and in a separate policy targeting the Android devices. Devices on the same platform can receive the same app configuration policy through group assignment, so additional policies are not required merely because there is more than one device. The number is determined by the supported platform-specific policy types needed for the managed devices. Microsoft's overview of app configuration policies explains the managed-device scenario and platform selection in the policy creation workflow. Microsoft also documents the iOS/iPadOS managed-device policy process separately, reflecting that these configurations are platform-specific. See App configuration policies for Microsoft Intune and Add app configuration policies for managed iOS/iPadOS devices.

## QUESTION NO: 52

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

**A.** Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.

**B.** Enable the Windows Firewall: Allow inbound remote administration exception setting.

**C.** Enable the Allow remote server management through WinRM setting.

**D.** Enable the Windows Firewall: Allow inbound Remote Desktop exceptions setting.

**E.** Enable the Allow Remote Shell access setting.

**F.** Set the Startup Type of the Remote Registry service to Automatic.

**ANSWER: A B C**

**Explanation:**

Setting the Startup Type of the Windows Remote Management (WS-Management) service to Automatic ensures that the WinRM service starts on every domain-joined device when it starts. This provides the Windows service infrastructure that receives and processes WS-Management requests, without requiring an administrator to configure each computer individually.

Enabling the Allow remote server management through WinRM setting configures the WinRM service through policy and specifies the IPv4 and IPv6 filters from which the device accepts remote management requests. This is the Group Policy setting used to allow remote management of the target computers through WinRM.

Enabling the Windows Firewall: Allow inbound remote administration exception setting provides the firewall exception needed for centrally managed inbound administrative connectivity. WinRM requires an inbound firewall allowance in addition to having the service running and configured; the service alone does not make remote connections possible. Applying these policies to an organizational unit containing the 200 computers provides a scalable domain-based deployment. Microsoft describes WinRM as the Microsoft implementation of WS-Management and documents its service, listener, and firewall configuration requirements in Installation and configuration for Windows Remote Management. See also Windows Remote Management.

## QUESTION NO: 53

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have 50 macOS devices enrolled in Intune.

You need to deploy an internally developed application named App1 to the devices. App1 is packaged as a signed PKG file.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create a macOS line-of-business app and upload the PKG file.

**B.** Assign App1 as Required to a device group.

**C.** Create a Windows app (Win32) app.

**D.** Approve App1 in Managed Google Play.

**E.** Create an iOS/iPadOS app provisioning profile.

## ANSWER: A B

**Explanation:**

Creating a **macOS line-of-business app** is required to upload and configure the signed PKG installer in Intune. Intune supports PKG files for macOS line-of-business app deployments.

After the app is configured, assigning **App1 as Required** to the device group causes Intune to install the app on the targeted enrolled Macs. Assigning the app as Available would require users to install the app from Company Portal instead. A Windows app (Win32) app type and Managed Google Play are not used for macOS PKG deployments. See Add macOS line-of-business apps to Microsoft Intune and Assign apps to groups with Microsoft Intune.

## QUESTION NO: 54

You have an Azure AD tenant named contoso.com.

You plan to purchase 25 computers that run Windows 11. You plan to deliver the computers directly to users.

You need to ensure that during the out-of-box experience (OBE), users are prompted to sign in, and then the computers are configured to use

Microsoft Intune.

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** a provisioning package

**B.** automatic enrollment

**C.** an unattend.xml answer file

**D.** a Windows Autopilot deployment profile for self-deploying mode

**E.** a Windows Autopilot deployment profile for user-driven mode

**ANSWER: B E**

**Explanation:**

**automatic enrollment** and **a Windows Autopilot deployment profile for user-driven mode** provide the required direct-to-user deployment experience. Automatic enrollment is configured in Microsoft Entra ID mobility settings and causes eligible Windows devices to enroll into Microsoft Intune automatically when a user signs in with their organizational account and the device is joined to Microsoft Entra ID. This establishes Intune management without requiring users to manually perform a separate enrollment process.

A Windows Autopilot deployment profile for user-driven mode is designed for devices that are shipped directly to users. When the user starts a registered device during the Windows out-of-box experience, they are prompted to authenticate using their work or school credentials. Autopilot then applies the deployment profile, joins the device to the organization as configured, and invokes automatic Intune enrollment. Intune can subsequently deliver required applications, configuration profiles, compliance settings, and security policies during enrollment. This combination therefore meets both requirements: user sign-in during OOBE and automatic configuration for Intune management. For implementation details, see Windows Autopilot user-driven mode and Enroll Windows devices in Intune.

**QUESTION NO: 55 - (SIMULATION)**

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

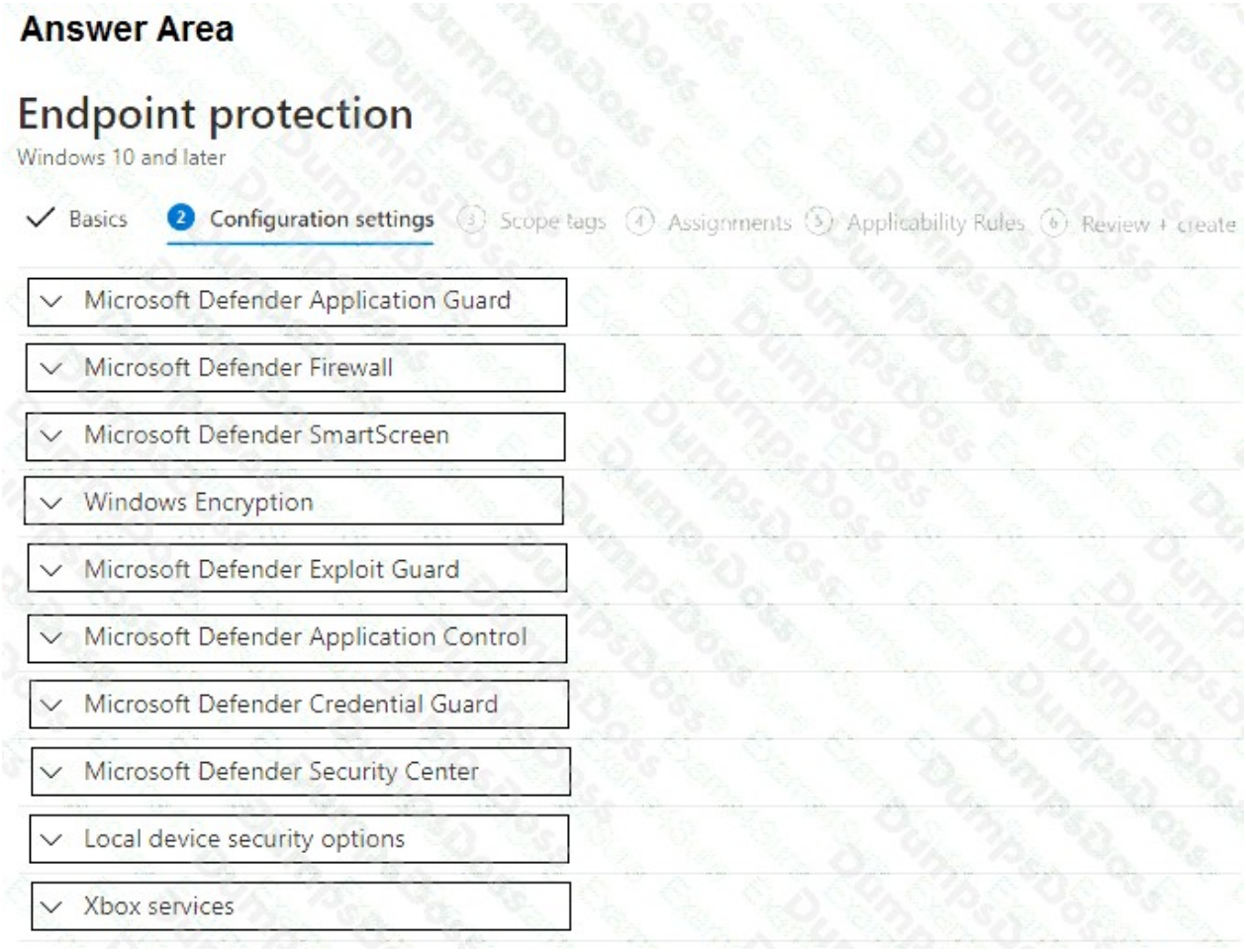
You need to configure an Intune device configuration profile to meet the following requirements:

Prevent Microsoft Office applications from launching child processes.

Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.




**ANSWER: See the explanation for the answer**

**Explanation:**

Configure the following two Endpoint protection areas:

**Microsoft Defender Exploit Guard** → **Attack surface reduction rules**: set **Block all Office applications from creating child processes** to **Enabled/Block**.

**Microsoft Defender Firewall**: create an **outbound block** firewall rule for **FTP** (TCP port `21`). Blocking the FTP control port prevents users from establishing FTP file-transfer sessions.

Thus, the two settings to select are **Microsoft Defender Exploit Guard** and **Microsoft Defender Firewall**.

## QUESTION NO: 56

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to deploy user certificates to Windows devices by using the Simple Certificate Enrollment Protocol (SCEP).

Which two certificate profiles should you create and assign? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** a trusted certificate profile

**B.** a SCEP certificate profile

**C.** a PKCS certificate profile

**D.** a device compliance policy

**E.** an app configuration policy

**ANSWER: A B**

**Explanation:**

A **trusted certificate profile** deploys the trusted root certificate that establishes trust in the certification authority that issues the SCEP certificates. Devices require this trust chain to validate certificates issued by the enterprise certification authority.

A **SCEP certificate profile** requests and deploys the identity certificate to the user or device by using the configured SCEP infrastructure. The SCEP profile references the trusted root certificate profile and defines certificate properties such as the subject name, key usage, and certificate template. A PKCS certificate profile is an alternative certificate-enrollment method, not a required companion to SCEP. See Configure SCEP certificate profiles in Microsoft Intune and Configure trusted certificate profiles in Microsoft Intune.

## QUESTION NO: 57

An employee reports that she must perform a BitLocker recovery on her laptop. The employee does not have her BitLocker recovery key but does have a Windows 10 desktop computer.

What should you instruct the employee to do from the desktop computer?

**A.** Run the manage-bde.exe “status command

**B.** From BitLocker Recovery Password Viewer, view the computer object of the laptop

**C.** Go to https://account.activedirectory.windowsazure.com and view the user account profile

**D.** Run the Enable-BitLockerAutoUnlock cmdlet

**ANSWER: C**

**Explanation:**

Go to https://account.activedirectory.windowsazure.com and view the user account profile is the appropriate self-service approach when the laptop’s BitLocker recovery key was backed up to the organization’s Microsoft Entra ID tenant. Using a separate, functioning Windows computer, the employee can authenticate with the same work or school account used on the affected device and access the device information associated with that identity. The recovery-key entry identifies the BitLocker recovery password needed to unlock the laptop, allowing the employee to enter the 48-digit password at the BitLocker recovery screen.

Microsoft Entra ID can escrow BitLocker recovery keys for Microsoft Entra joined or registered devices, particularly in cloud-managed environments. Microsoft’s current user-facing experience is available through the My Account portal; the legacy account portal URL in the question represents this organizational account-management path. The employee must be able to sign in and the key must previously have been successfully backed up to Microsoft Entra ID. For the current steps to locate a key, see Finding your BitLocker recovery key. Administrators can also view escrowed keys as documented in View or copy BitLocker keys in Microsoft Entra ID.

## QUESTION NO: 58

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?

**A.** On Computer2, run the Enable-PSRemoting cmdlet.

**B.** On Computer2, add Computer1 to the Remote Management Users group.

**C.** From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.

**D.** On Computer1, run the HcK-PSSession cmdlet.

**ANSWER: A**

**Explanation:**

On Computer2, run the Enable-PSRemoting cmdlet. `Invoke-Command` executes commands on a remote computer through PowerShell remoting. Before Computer1 can use `Invoke-Command` to run commands remotely on Computer2, the target computer must be configured to receive PowerShell remoting connections. `Enable-PSRemoting` performs the required initial configuration: it starts and configures the Windows Remote Management (WinRM) service, creates a PowerShell remoting endpoint/session configuration, and enables the necessary inbound firewall rules for WS-Management traffic. In an Active Directory domain, the domain profile firewall rules created by this cmdlet support communication from domain-connected management devices, assuming ordinary network connectivity and appropriate user permissions. After remoting is enabled on the target, an authorized user on Computer1 can use `Invoke-Command -ComputerName Computer2` to execute one or more commands remotely. Microsoft documents that PowerShell remoting is enabled by using `Enable-PSRemoting`, and that `Invoke-Command` uses remoting to run commands on local or remote computers. See Enable-PSRemoting documentation and Invoke-Command documentation.

## QUESTION NO: 59

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have 100 Windows 11 devices enrolled in Intune.

You need to reduce the risk of malware by preventing Microsoft Office applications from creating child processes on the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A.** Create an attack surface reduction rules policy for Windows 10 and later.

**B.** Configure Block all Office applications from creating child processes to Block.

**C.** Create an antivirus policy.

**D.** Create an app protection policy.

**E.** Create an endpoint detection and response policy.

**ANSWER: A B**

**Explanation:**

Create an **attack surface reduction rules policy** for Windows 10 and later. Attack surface reduction policies include the Microsoft Defender rule that blocks Office applications from creating child processes. This rule can help prevent malicious documents from using Office applications to launch processes such as command shells or script hosts.

Configure the **Block all Office applications from creating child processes** rule to Block and assign the policy to the applicable device group. An antivirus policy configures antivirus settings, while an app protection policy protects organizational data in supported apps and does not configure Windows Defender attack surface reduction rules. See Attack surface reduction rules policy in Intune and Attack surface reduction rules reference.

## QUESTION NO: 60

What should you configure to meet the technical requirements for the Azure AD-joined computers?

**A.** Windows Hello for Business in the Microsoft Intune admin center.

**B.** The Accounts options in an endpoint protection profile.

**C.** The Password Policy settings in a Group Policy object (GPO).

**D.** A password policy from the Microsoft Office 365 portal.

**ANSWER: A**

**Explanation:**

Windows Hello for Business in the Microsoft Intune admin center is the appropriate configuration for Microsoft Entra ID-joined Windows computers when the requirement is to provide secure, passwordless interactive sign-in. Windows Hello for Business uses asymmetric cryptography: the device retains a protected private key while the corresponding public key is registered with the identity provider. A user unlocks the private key through a local gesture, such as a PIN, fingerprint, or facial recognition. The PIN is device-specific rather than a reusable network credential, helping protect against phishing and credential replay.

For cloud-managed endpoints, Intune provides policy settings that enable Windows Hello for Business and define the organization's required experience, including PIN rules, biometric authentication, enhanced anti-spoofing where supported, and security-key-related controls. These settings are delivered through Windows enrollment and device configuration policies, making Intune the management plane that applies the sign-in requirements consistently to the joined computers. Microsoft documents Windows Hello for Business as a passwordless authentication method for Windows and documents its Intune policy management in the Windows Hello for Business overview and Account protection policies in Intune.

**QUESTION NO: 61**

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

| Name | Operating system | Role |
|---|---|---|
| DC1 | Windows Server 2019 | Domain controller |
| Server1 | Windows Server 2016 | Member server |
| Server2 | Windows Server 2019 | Member server |

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

ADatum has a hybrid Azure AD tenant named adatum.com. Users and Groups -

| Name | Azure AD role | Member of |
|---|---|---|
| User1 | Cloud Device Administrator | GroupA |
| User2 | Azure AD Joined Device Local Administrator | GroupB |
| User3 | Global Reader | GroupA, GroupB |
| User4 | Global Administrator | Group1 |

The adatum.com tenant contains the users shown in the following table.

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license. Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

| Name | Type | Member of | Scope (Tags) |
|---|---|---|---|
| Device1 | Corporate-owned | Group1 | Default |
| Device2 | Corporate-owned | Group1, Group2 | Tag2 |
| Device3 | Personally-owned | Group1 | Tag1 |
| Device4 | Personally-owned | Group2 | Tag2 |
| Device5 | Corporate-owned | Group3 | Default |

ADatum has the Windows 10 devices shown in the following table.

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune. The Windows 10 devices are configured as shown in the following table.

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1. Microsoft Intune Configuration -

| Name | Configuration | Assignment |
|---|---|---|
| Policy1 | Require BitLocker only | Group1 |
| Policy2 | Require Secure Boot only | Group1 |
| Policy3 | Require BitLocker and Secure Boot | Group2 |

Microsoft Intune has the compliance policies shown in the following table.

**The Compliance policy settings are shown in the following exhibit.**

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as: Compliant / Not Compliant

Enhanced jailbreak detection: Enabled / Disabled

Compliance status validity period (days): 30

The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA - MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings: Name: Protection1 -

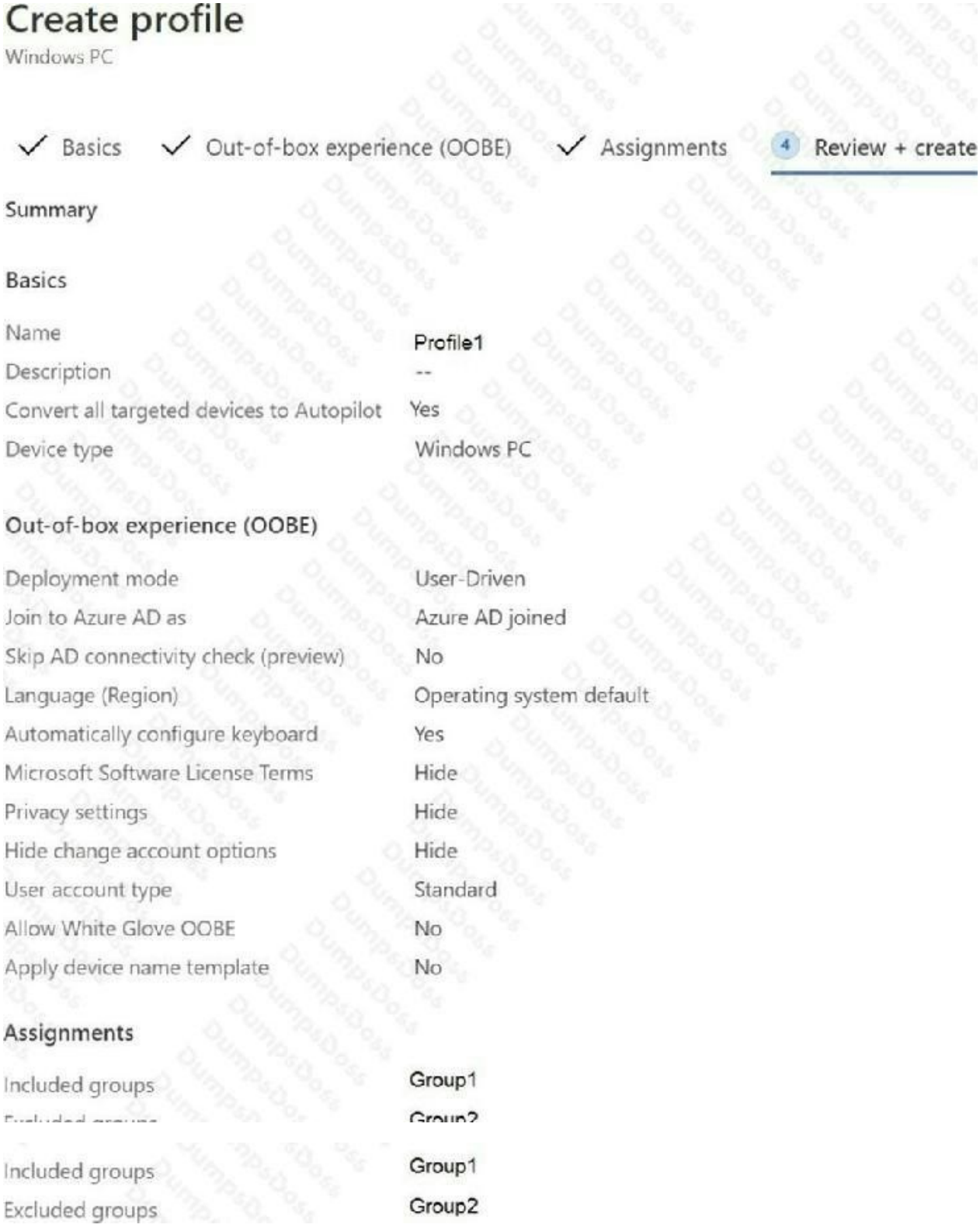
Folder protection: Enable -

List of apps that have access to protected folders: C:*\AppA.exe List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB - Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.




Currently, there are no devices deployed by using Windows Autopilot. The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

Purchase a new Windows 10 device named Device6 and enroll the device in Intune

New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined. Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 - Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings: Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP - Assignments:

Included groups: Group1, Group2, GroupA Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 - Assignments:

Included groups: GroupA - Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements: Users in GroupA must be able to deploy new computers. Administrative effort must be minimized.

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

**A.** Device2 only

**B.** Device3 only

**C.** Device1, Device2, and Device5 only

**D.** Device1, Device2, Device3, and Device4 only

**ANSWER: D**

**Explanation:**

Device1, Device2, Device3, and Device4 only receive the 192.168.1.0/24 network boundary because Boundary1 is assigned to Group1 and Group2. Intune deploys a configuration profile according to its group assignments. Based on the users and devices shown in the case-study tables, Device1 through Device4 fall within the assignment targeting produced by those two included groups, so each receives the profile's network-boundary setting.

The Tag1 scope tag on Boundary1 does not alter this result. Scope tags are an Intune role-based access control feature: they limit the Intune objects that delegated administrators can view or manage. A scope tag is therefore administrative metadata, rather than a deployment assignment or device filter. The profile is delivered because of the included Group1 and Group2 assignments, not because a device or user has Tag1.

Microsoft's Intune documentation distinguishes profile assignment from RBAC scoping: configuration profiles are deployed by assigning them to Microsoft Entra user or device groups, while scope tags are used to control administrator visibility and management scope. This makes the listed four devices the complete set to which Boundary1 applies. See Assign device profiles in Microsoft Intune and Use scope tags to filter policies.

**QUESTION NO: 62**

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

**A.** From Platform Settings, set Android device administrator Personally Owned to Block.

**B.** From Platform Settings, set Android Enterprise (work profile) to Allow.

**C.** From Platform Settings, set Android device administrator Personally Owned to Allow

**D.** From Platform Settings, set Android device administrator to Block.

**ANSWER: A B**

**Explanation:**

“From Platform Settings, set Android device administrator Personally Owned to Block.” and “From Platform Settings, set Android Enterprise (work profile) to Allow.” together enforce the intended personally owned Android enrollment method. Intune enrollment restrictions evaluate the permitted platform and enrollment type before a device can be enrolled. Allowing Android Enterprise work profile enables the personally owned Android Enterprise enrollment flow, which creates a separate, managed work profile for organizational apps, accounts, and data while leaving the user’s personal profile independently managed.

Blocking personally owned Android device administrator enrollment prevents users from using the legacy Android device administrator method for personal devices. This ensures that a personally owned device cannot enroll through that alternative management path and instead must use the Android Enterprise work profile method that the organization requires. The restriction therefore both permits the approved Android enrollment experience and prevents the legacy personally owned enrollment experience.

Microsoft documents platform-specific enrollment controls in Set enrollment restrictions in Microsoft Intune. For the work-profile enrollment model and its separation of work and personal data, see Set up enrollment for personally owned Android Enterprise work profile devices.

**QUESTION NO: 63**

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune.

You create an app configuration policy that contains the following settings:

• Device enrollment type: Managed devices

• Profile Type: All Profile Types

• Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** Android Enterprise system app

**B.** Web link

**C.** Android store app

**D.** Managed Google Play store app

**E.** Built-in Android app

**ANSWER: A D**

**Explanation:**

**Android Enterprise system app** and **Managed Google Play store app** can be associated with an Android Enterprise app configuration policy for managed devices. Intune app configuration policies deliver managed configuration values to an app through the Android Enterprise managed-configuration framework. Selecting *Managed devices*, *Android Enterprise*, and *All Profile Types* makes the policy applicable across supported Android Enterprise enrollment profiles, subject to the selected app's support for managed configurations.

Managed Google Play is the Android Enterprise enterprise app catalog integrated with Intune. After an administrator approves and synchronizes an app, Intune can target that managed Google Play app and send configuration keys defined by the app developer. This allows settings such as server addresses, account behavior, feature controls, and other organization-specific values to be deployed without user input.

Android Enterprise system apps can also be selected when the relevant system app supports managed configurations. These are apps included on the device image that are identified and managed through their Android package name; Intune can associate configuration policy settings with the supported system application in Android Enterprise scenarios. Microsoft documents this Android Enterprise app-configuration workflow at Use app configuration policies for Android Enterprise and documents Android Enterprise app management, including Managed Google Play integration, at Add Managed Google Play apps to Android Enterprise devices with Intune.

## QUESTION NO: 64 - (DRAG DROP)

DRAG DROP -

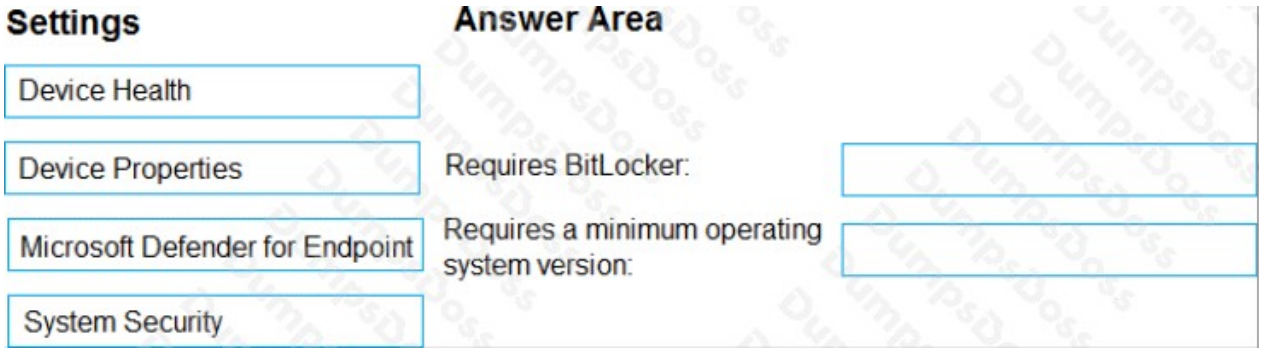
You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

Requires BitLocker Drive Encryption (BitLocker) on each device Requires a minimum operating system version

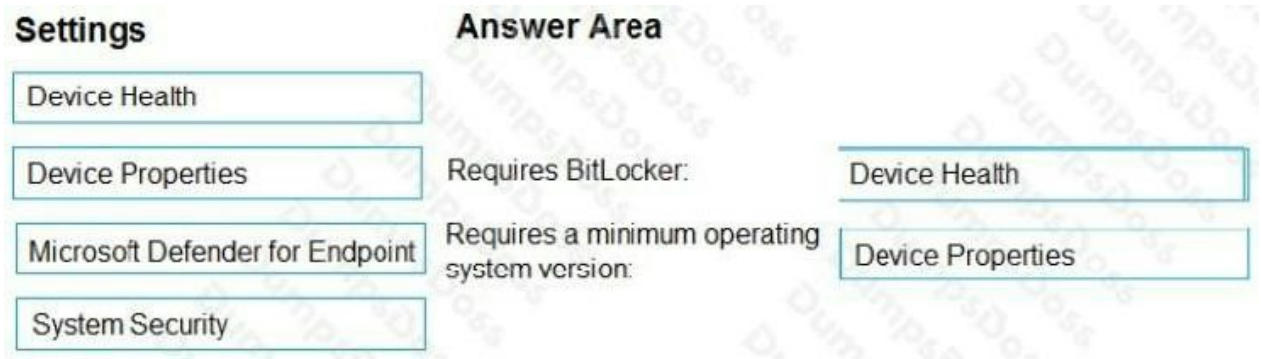
Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct

requirements. Each setting 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.

NOTE: Each correct selection is worth one point.




## ANSWER:




**Explanation:**

In an Intune compliance policy for Windows, **Device Health** is the correct setting category for requiring BitLocker Drive Encryption. Compliance policies use this category to evaluate key security-health conditions that a Windows device must satisfy before it can be reported as compliant. The BitLocker requirement checks whether the device's drive encryption protection is enabled. This lets an organization ensure that data stored locally on managed devices is protected if a device is lost, stolen, or accessed outside of approved circumstances. Intune evaluates the reported encryption state as part of the device compliance assessment and can mark a device noncompliant when it does not meet the configured BitLocker requirement. Microsoft documents the BitLocker compliance check under the Windows Device Health settings in its Windows compliance settings reference.

**Device Properties** is the correct category for a minimum operating system version. The installed operating-system version is a characteristic of the device that Intune inventories and compares with the minimum version value configured in the compliance policy. Defining a minimum version helps ensure devices have reached an organization's required Windows release or build baseline, including the updates and platform capabilities associated with that baseline. During compliance evaluation, Intune compares the version reported by the enrolled device to the configured minimum operating-system version. Devices that meet or exceed that configured threshold satisfy this requirement. This policy evaluation can be used with Conditional Access, allowing access decisions to incorporate whether a device meets both encryption and operating-system baseline requirements. Microsoft explains the purpose and behavior of compliance policies in the Intune device compliance policy overview.

## QUESTION NO: 65

You have a Microsoft 365 E5 subscription.

You have a Microsoft Intune enrollment profile for Android Enterprise devices that has the following settings:

• Name: Profile1

• Token type: Corporate-owned, fully managed

You need to enroll a new Android device in Intune by using Profile1. What should you use to enroll the device?

**A.** a QR code

**B.** the Microsoft Authenticate app

**C.** the Intune app

**D.** the Company Portal app

## ANSWER: A

**Explanation:**

**a QR code** is the appropriate enrollment method for an Android Enterprise corporate-owned, fully managed device. In the Intune admin center, the enrollment profile provides a token that can be used to generate a QR code. During the device's initial Android setup experience, the administrator or user starts QR-code provisioning and scans that generated code. The scan downloads and applies the Android Device Policy controller, associates the device with the Intune tenant and the selected enrollment profile, and continues the fully managed enrollment process.

Corporate-owned, fully managed mode is intended for organization-owned devices that are managed across the entire device, rather than only within a work profile. QR-code provisioning is therefore a supported and practical method for onboarding a new device directly from its out-of-box setup flow. The QR code is tied to the enrollment token, so using the token generated for Profile1 ensures that the device is enrolled with that profile's corporate-owned, fully managed configuration. Microsoft documents QR-code enrollment as a supported provisioning method for Android Enterprise fully managed devices. See Enroll Android Enterprise fully managed devices and Enroll Android devices.

## QUESTION NO: 66

You have several computers that run Windows 10. The computers are in a workgroup. You need to prevent users from using Microsoft Store apps on their computer.

What are two possible ways to achieve the goal? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

**A.** From Security Settings in the local Group Policy, configure Security Options.

**B.** From Administrative Templates in the local Group Policy, configure the Store settings.

**C.** From Security Settings in the local Group Policy, configure Software Restriction Policies.

**D.** From Security Settings in the local Group Policy, configure Application Control Policies.

**ANSWER: B D**

**Explanation:**

From Administrative Templates in the local Group Policy, configure the Store settings is a valid method because Local Group Policy includes Microsoft Store policies under Windows Components. In particular, the policy to turn off the Store application prevents users from opening Microsoft Store. Because the devices are in a workgroup, the policy can be configured directly on each device through the Local Group Policy Editor; Active Directory domain membership is not required.

From Security Settings in the local Group Policy, configure Application Control Policies is also valid because this area contains AppLocker policy collections. AppLocker can create packaged-app rules that apply to Microsoft Store apps and packaged app installers. An administrator can use these rules to allow or deny specified packaged apps for users or groups, thereby preventing the targeted Store apps from running. AppLocker enforcement requires a Windows edition that supports AppLocker enforcement, such as Windows Enterprise or Education. Microsoft documents Store access controls at Configure access to Microsoft Store and documents packaged-app controls at Packaged apps and packaged app installers in AppLocker.