DUMPSBOSS.

Endpoint Administrator

Microsoft MD-102

Version Demo

Total Demo Questions: 50

Total Premium Questions: 504

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Prepare infrastructure for devices	142
Topic 2, Manage and maintain devices	148
Topic 3, Manage applications	60
Topic 4, Protect devices	114
Topic 5, Case Study Contoso, Ltd.	30
Topic 6, Case Study Litware inc	10
Total	504

QUESTION NO: 1

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to use Intune to deploy an application named App1 that contains multiple installation files.

What should you do first?

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

B. Create an Android application package (APK).

C. Upload the contents of App1 to Intune.

D. Install the Microsoft Deployment Toolkit (MDT).

ANSWER: A

Explanation:

Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool is correct because Intune requires Windows Win32 apps to be packaged into the .intunewin format before they can be uploaded and deployed. When an application has multiple installation files, you place all required files in a source folder and then run the Microsoft Win32 Content Prep Tool against that folder, specifying the setup file and output location. The tool compresses and encrypts the app content into a single .intunewin package that Intune can accept as a Win32 app. After this packaging step is complete, you can create the Win32 app in the Microsoft Intune admin center, upload the generated .intunewin file, and configure install commands, detection rules, requirements, and assignments. Microsoft's documentation describes this as the required preparation step for Win32 app management in Intune. See Prepare Win32 app content for upload and Add, assign, and monitor a Win32 app in Microsoft Intune.

QUESTION NO: 2

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution; You use the Microsoft Authenticator app.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. Microsoft Entra device registration is the process of creating a device identity in the tenant so that Microsoft Entra ID can recognize the device and use it for scenarios such as Conditional Access and single sign-on to organizational resources. For personally owned mobile devices, including Android, this can be initiated through the Microsoft Authenticator app when a user adds or signs in with a work or school account and completes the device registration flow. The result is that the Android device becomes registered with the Microsoft Entra tenant, which satisfies the requirement to register Device1 in

contoso.com. This is different from full mobile device management enrollment in Microsoft Intune, which typically uses the Company Portal app and applies management policies. The stated goal is only Microsoft Entra registration, not Intune enrollment, so using Microsoft Authenticator meets the goal. Microsoft describes Microsoft Entra registered devices as identities for user-owned devices such as Android devices, and Microsoft support guidance documents registering a personal Android device to a work or school network through the Authenticator-based registration experience. See Microsoft Entra registered devices and Register your personal device on your work or school network.

QUESTION NO: 3

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:

For an Intune app configuration policy where the device enrollment type is Managed devices and the platform is Android Enterprise, the policy is associated with Android Enterprise app types that Intune can manage on enrolled devices. Managed Google Play store app is correct because Android Enterprise app deployment in Intune is centered on apps approved and synchronized from Managed Google Play, and these apps can expose managed configuration settings that Intune delivers through app configuration policies. Android Enterprise system app is also correct because Intune supports Android Enterprise system apps as a distinct app type for Android Enterprise scenarios, allowing administrators to enable and manage supported system applications on enrolled Android Enterprise devices. When creating Android Enterprise app configuration policies for managed devices, Intune lets admins select the applicable profile type, such as all Android Enterprise profile types, and then associate the policy with a supported Android Enterprise app. Microsoft documents Android Enterprise app configuration policy behavior and managed configuration support in Use app configuration policies for Android Enterprise and describes Android Enterprise app management through Managed Google Play in Add Managed Google Play apps to Android Enterprise devices with Intune.

QUESTION NO: 4

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:

To assign the same Windows Autopilot deployment profile to every device registered for Autopilot, the correct approach is to first create an Azure AD group that has dynamic membership rules and uses the ZTDID tag. Autopilot-registered devices have a physical ID value that includes the ZTDId marker, so a dynamic device group can automatically include all Windows Autopilot devices without requiring manual group updates. Microsoft's guidance commonly uses a rule such as device.devicePhysicalIDs -any (_ -contains "[ZTDId]") for this purpose.

After the Autopilot devices are collected in that dynamic group, assign a Windows Autopilot deployment profile to a group. Autopilot deployment profiles are targeted through Microsoft Intune group assignments, so assigning the profile to the dynamic Autopilot device group ensures that all current and future Autopilot-registered computers receive the same deployment profile automatically. This is the standard scalable method for applying a consistent Autopilot configuration across enrolled devices. For reference, see Microsoft's documentation on creating an Autopilot device group and Autopilot deployment profiles.

QUESTION NO: 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that

might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because Microsoft Entra user and device settings do not control the Windows Hello for Business PIN complexity requirement. Those tenant-level settings are used for identity and device registration behaviors, such as whether users can join devices to Microsoft Entra ID, whether multifactor authentication is required for device join, and who becomes a local administrator on joined devices. They do not define the minimum PIN length that users must configure during Windows Hello for Business provisioning.

To require a six-digit PIN, the organization must configure a Windows Hello for Business policy that includes the minimum PIN length setting. In Microsoft Intune, this is commonly configured under Windows enrollment settings for Windows Hello for

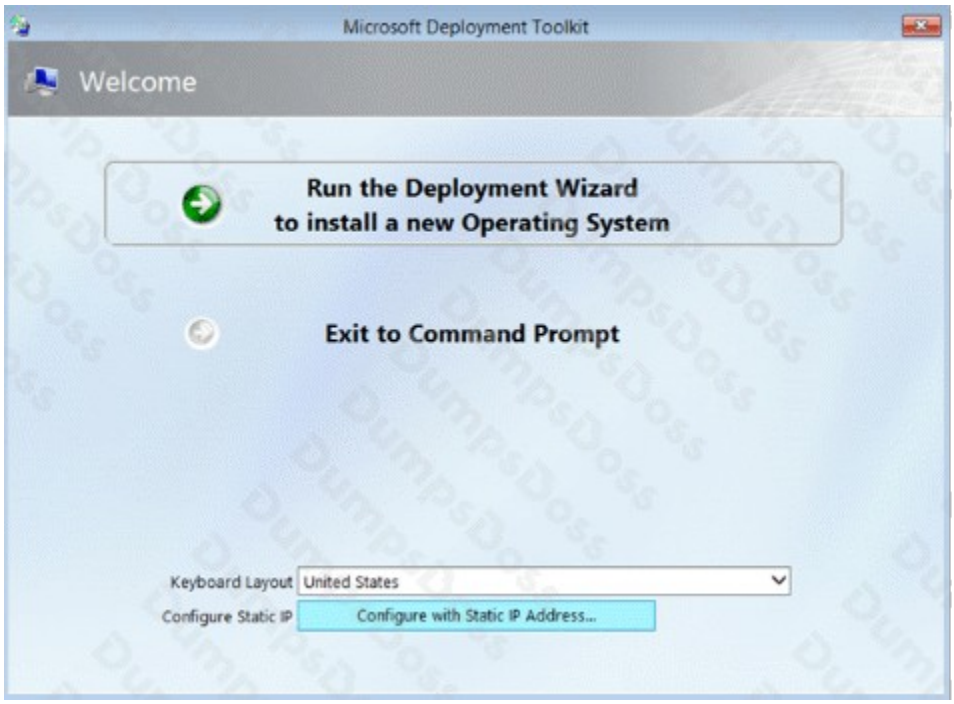
Business or by using a device configuration/account protection policy that sets Windows Hello for Business PIN requirements. Microsoft documents the available Windows Hello for Business PIN settings, including minimum PIN length, and Intune's Windows Hello for Business policy options. See Windows Hello for Business policy settings and Configure Windows Hello for Business in Intune.

QUESTION NO: 6 - (DRAG DROP)

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

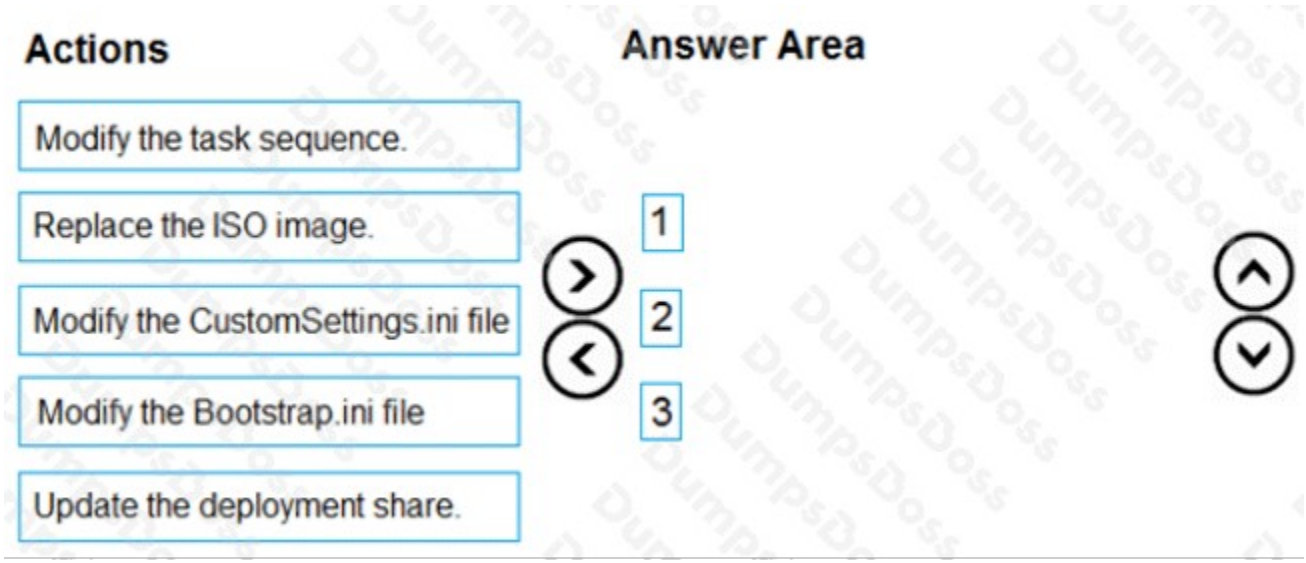
When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.



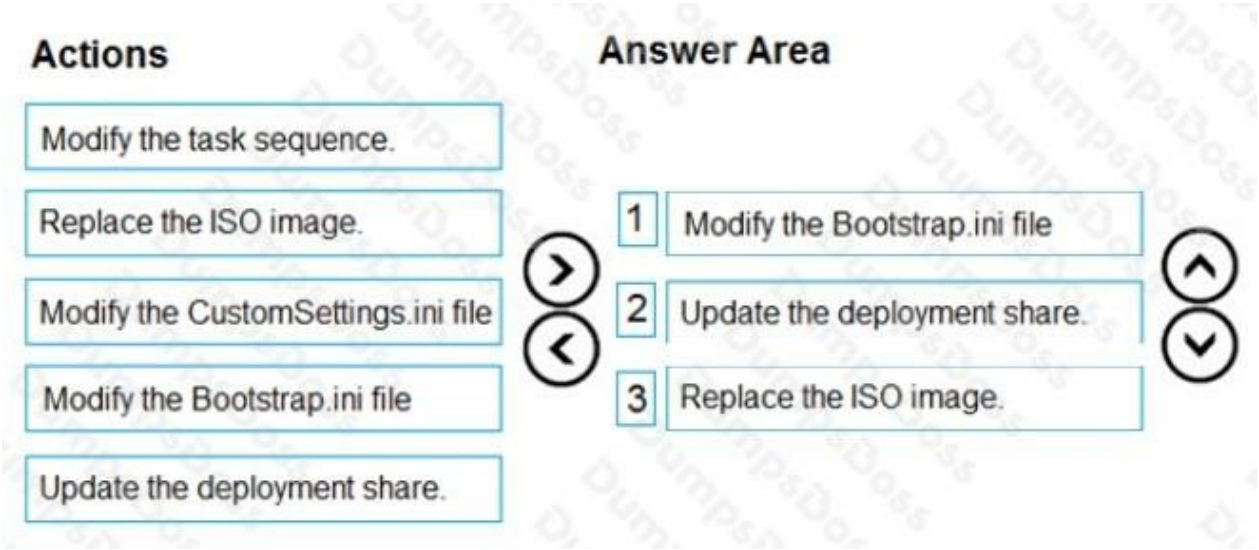
You need to prevent the welcome screen from appearing when the computers connect to MDT1.

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:

To stop the Microsoft Deployment Toolkit Lite Touch welcome screen from appearing, the change must be made in the bootstrapping configuration that is loaded before the deployment wizard starts. The relevant file is **Bootstrap.ini**, which is used by the Lite Touch Windows PE environment to find and connect to the deployment share and to control early wizard behavior. Setting **SkipBDDWelcome=YES** in this file suppresses the initial MDT welcome page shown in the exhibit, allowing the deployment process to continue without presenting that welcome screen to the technician or user.

After modifying **Bootstrap.ini**, MDT does not automatically inject that change into existing boot media. The LiteTouchPE_x64.iso file already contains the previous bootstrap configuration, so the deployment share must be updated. Updating the deployment share regenerates the Lite Touch boot images and ISO files so that the edited Bootstrap.ini settings are included in the Windows PE media. Microsoft's MDT deployment guidance describes this update process as part of maintaining generated Lite Touch boot media; see Deploy a Windows image using MDT and the MDT documentation entry point at Microsoft Deployment Toolkit documentation.

Because the computers in the scenario are starting from **LiteTouchPE_x64.iso**, the final required step is to replace the currently used ISO with the newly generated ISO from the updated deployment share. Only then will newly booted computers load the updated Bootstrap.ini configuration and bypass the welcome screen.

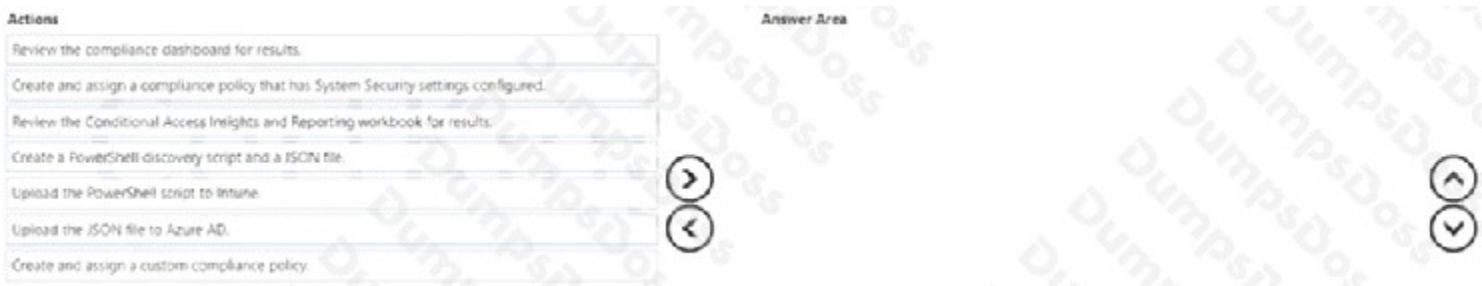
QUESTION NO: 7 - (DRAG DROP)

DRAG DROP

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

Which four 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:

To validate a BIOS version with Microsoft Intune, the correct approach is to use Windows custom compliance settings. Custom compliance relies on a PowerShell discovery script to inspect the device and return the value being evaluated, and a JSON rules file to define how Intune should interpret that returned value. In this scenario, the discovery script would query the BIOS version from the Windows device, and the JSON rule would define the expected value or condition that determines whether the device is compliant. Microsoft documents this workflow for custom compliance policies, where you first prepare the discovery script and JSON rule definition, then add the script to Intune so it can be selected during policy creation. See Microsoft's guidance on custom compliance settings in Intune.

After the script is available in Intune, you create and assign a custom compliance policy for Windows devices. During that policy configuration, the custom compliance rule definition is associated with the policy, and the policy is assigned to the target device or user groups. Once devices evaluate the policy, Intune records the compliance state and exposes it through compliance reporting. Because the question explicitly asks to create and monitor the results, the final action should be to review the compliance dashboard for the results after the policy has been assigned and devices have checked in. Microsoft describes policy reporting and compliance status review in its documentation for monitoring device compliance policies in Intune. This sequence matches the Intune custom compliance lifecycle: define the detection and rule logic, upload the discovery script, create and assign the custom compliance policy, and then review compliance reporting.

QUESTION NO: 8

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

A. General

B. Users and Accounts

C. System security

D. Device experience

ANSWER: D

Explanation:

Device experience is the correct configuration area because Intune exposes Android Enterprise kiosk behavior through the device restrictions profile settings in that section. For a single-app kiosk configuration, the administrator uses the kiosk-related controls to define the kiosk mode and specify the app that the device is allowed to run. This is the Intune setting group designed for controlling the end-user device experience, including locking the device into one managed app or configuring a more controlled multi-app experience, depending on the Android Enterprise kiosk scenario. Microsoft's Android Enterprise device restrictions documentation identifies the Device experience settings as the place where kiosk mode options are configured, including single-app kiosk settings. In practice, the app should also be properly deployed or available as a managed Google Play app so the device can launch it reliably in kiosk mode. See Microsoft Learn for the Android Enterprise device restrictions settings and kiosk configuration guidance: Android Enterprise device restrictions - Device experience and Set up Android Enterprise dedicated device management.

QUESTION NO: 9

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:

To let User1 initiate a Remote Help session for Device1 from the Intune admin center, Device1 must have the Remote Help app available, User1 must have the appropriate Intune RBAC permissions, and User1 must be licensed for Remote Help. Deploying the Remote Help app to Device1 is required because Remote Help sessions rely on the app being installed on the device that participates in the support session. Assigning the Help Desk Operator role to User1 is appropriate because helpers need Intune role-based access control permissions that allow them to perform Remote Help actions from the admin center. Assigning the Remote Help add-on license to User1 provides the Remote Help entitlement required for helpers; Remote Help can also be licensed through Microsoft Intune Suite, but the key requirement is that the user has a Remote Help-capable license in addition to base Intune licensing. Microsoft documents these requirements in the Remote Help prerequisites and configuration guidance for Intune. See Use Remote Help with Microsoft Intune and Role-based access control with Microsoft Intune.

QUESTION NO: 10

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in

Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender for Endpoint.

What should you do?

A. From the Microsoft Intune admin center, create an attack surface reduction (ASR) policy.

B. From the Microsoft 365 Defender portal, enable tamper protection.

C. From the Microsoft Intune admin center, create an account protection policy.

D. From the Microsoft Entra admin center, create a Conditional Access policy.

ANSWER: B

Explanation:

From the Microsoft 365 Defender portal, enable tamper protection is correct. Tamper protection is specifically designed to prevent unauthorized changes to Microsoft Defender security settings on endpoints. When enabled, it helps stop users, malware, or unauthorized processes from turning off important Microsoft Defender Antivirus capabilities such as real-time protection, cloud-delivered protection, behavior monitoring, and other core protections used with Microsoft Defender for Endpoint. In an enterprise environment, tamper protection can be enabled tenant-wide from the Microsoft Defender portal, which is the appropriate central location when managing Microsoft Defender for Endpoint settings across enrolled Windows devices. This aligns with the requirement to prevent users from disabling protection rather than simply configuring detection or access policies. Microsoft documents tamper protection as the feature used to lock down Defender Antivirus settings and prevent them from being changed outside supported management channels. See Microsoft's guidance on protecting security settings with tamper protection and the related tamper protection management options.

QUESTION NO: 11

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: B D

Explanation:

In Microsoft Intune, enrollment device platform restrictions are used to control which device platforms and enrollment methods are permitted to enroll. To allow only Android devices that enroll by using Android Enterprise work profiles, the Android Enterprise work profile enrollment path must be allowed, and the legacy Android device administrator enrollment path must be blocked. Therefore, "From Platform Settings, set Android Enterprise (work profile) to Allow" is required so that supported Android Enterprise work profile devices can enroll. "From Platform Settings, set Android device administrator to Block" is also required because Android device administrator is a separate Android enrollment method; leaving it allowed would permit Android devices to enroll without using Android Enterprise work profiles. Together, these settings ensure that Intune accepts the intended Android work profile enrollment scenario while preventing the alternative Android device administrator enrollment method. Microsoft documents these controls in the Intune enrollment device platform restrictions settings, and separately describes Android Enterprise personally owned work profile enrollment as the Android work profile enrollment method. See Microsoft Intune enrollment restrictions and Android Enterprise work profile enrollment.

QUESTION NO: 12

You have a Microsoft 365 subscription that contains Windows 11 devices enrolled in Microsoft Intune.

You need to use Device query to identify whether a critical security patch was installed on a device.

Which table should you target?

A. Fileinfo

B. OsVersion

C. WindowsQfe

D. SystemInfo

E. WindowsRegistry

ANSWER: C

Explanation:

WindowsQfe is correct because Device query in Microsoft Intune exposes device inventory through supported query tables, and the WindowsQfe table is specifically intended for Windows Quick Fix Engineering information. In practical terms, this is where Windows hotfix and update records are surfaced, including fields such as the installed update identifier, installation date, and related update metadata. A critical security patch installed through Windows Update is represented as a QFE/hotfix entry, commonly identified by its KB number, so querying WindowsQfe lets an administrator verify whether a particular security update is present on an enrolled Windows 11 device. This aligns with the way Intune Device query is used for near real-time investigation of endpoint state by running queries against device data collected from Windows devices. Microsoft documents Device query as a capability for querying device properties in Intune, and the WindowsQfe table is included among the supported schema tables for Windows update and hotfix information. See Device query in Microsoft Intune and the Device query schema for the supported table details.

QUESTION NO: 13

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:

To enable WinRM across domain-joined Windows 10 computers by using Group Policy, you need to configure the WinRM service, allow it to accept remote management requests, and permit the required inbound firewall traffic. Enabling the **Allow remote server management through WinRM** policy configures the WinRM service to listen for remote management requests and can define the IPv4 and IPv6 filters that are allowed to connect. Setting the **Windows Remote Management (WS-Management)** service startup type to **Automatic** ensures that the WinRM service starts reliably on each managed computer after policy is applied and after restarts. Enabling the **Windows Defender Firewall: Allow inbound remote administration exception** setting provides the firewall allowance needed for remote administration traffic so that management connections are not blocked by the local firewall. Together, these settings allow centralized WinRM enablement through Group Policy instead of manually running configuration commands on each computer. Microsoft documents the WinRM service configuration requirements, including listeners and firewall considerations, in its WinRM setup guidance: Installation and configuration for Windows Remote Management. The Group Policy setting for WinRM service management is also described in Microsoft's policy reference: Policy CSP - RemoteManagement.

QUESTION NO: 14

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:

Log Analytics can collect several standard monitoring data types from Windows 10 computers that are connected to a Log Analytics workspace. The average processor utilization is correct because Windows performance counters can be collected and stored in the workspace, including processor-related counters used to trend CPU usage across managed endpoints. Error events from the System log is also correct because Windows event logs are a supported data source; administrators can configure collection from logs such as System and filter by event level, including Error. Third-party application logs stored as text files is correct because Log Analytics supports custom log collection, allowing text-based application logs to be ingested and queried in the workspace when they meet the supported format and collection requirements. These capabilities align with the core Log Analytics agent data sources used for endpoint monitoring: performance counters, Windows event logs, and custom logs. See Microsoft's documentation on Log Analytics agent data sources and custom text log collection.

QUESTION NO: 15

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:

The usable provisioning options are **a custom Windows image**, **Windows Autopilot**, and **provisioning packages**. A custom Windows image can be built from Windows 11 Enterprise and customized before deployment to include required applications such as an MSI package and required certificates, then deployed as part of an organizational Windows deployment process. **Windows Autopilot** is also a complete modern provisioning approach for new Windows devices: it can join devices to Microsoft Entra ID, enroll them in Intune, and allow Intune to deliver required apps, certificates, and configuration profiles during provisioning. Microsoft documents Autopilot as a way to set up and pre-configure new devices so they are business-ready with minimal IT interaction: Windows Autopilot overview. **Provisioning packages** are another complete option because Windows Configuration Designer packages can be used to configure Windows devices without reimaging, including adding certificates, installing applications, applying edition upgrade settings, and joining devices to Microsoft Entra ID when configured for organizational use. Microsoft describes provisioning packages as a method for quickly configuring Windows client devices with settings, apps, and enrollment-related configuration: Provisioning packages for Windows.

QUESTION NO: 16

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:

The correct configurations are “From Platform Settings, set Android device administrator Personally Owned to Block.” and “From Platform Settings, set Android Enterprise (work profile) to Allow.” In Intune device enrollment restrictions, Android enrollment methods are controlled separately in the platform settings. Android Enterprise work profile enrollment is the supported enrollment path for personally owned Android devices when you want corporate data isolated in a managed work profile. Setting Android Enterprise (work profile) to Allow permits users to enroll Android devices through that work profile method. Setting Android device administrator Personally Owned to Block prevents personal Android devices from enrolling through the older Android device administrator management method, which would not create the Android Enterprise work profile experience you require. Together, these settings direct eligible Android enrollments to the Android Enterprise work profile flow while preventing the legacy personally owned Android device administrator enrollment path. Microsoft documents these controls under Intune enrollment device platform restrictions and Android Enterprise personally owned work profile enrollment. See Set enrollment restrictions in Microsoft Intune and Set up enrollment for personally owned Android Enterprise work profile devices.

QUESTION NO: 17

You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.

Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.

You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment

process. The solution must minimize the number of changes.

Which DNS records do you need?

A. one TXT record only

B. three CNAME records

C. three TXT records

D. one CNAME record only

ANSWER: B

Explanation:

three CNAME records is correct because Intune uses DNS CNAME discovery to locate the MDM enrollment service automatically from the user's sign-in UPN suffix. When a user enrolls a device, Windows checks the domain portion of the user name, such as contoso.com, us.contoso.com, or eu.contoso.com, and looks for the corresponding enterprise enrollment DNS alias. For Intune, that alias must point to the Intune enrollment service, typically EnterpriseEnrollment.manage.microsoft.com or the documented Intune enrollment target used by the tenant. Because users sign in with three different suffixes, each suffix needs its own CNAME record so enrollment discovery succeeds regardless of which UPN suffix the user enters.

This is the minimal required DNS-based change to prevent users from manually entering the MDM enrollment URL during enrollment. Microsoft documents this CNAME-based approach for simplifying Windows device enrollment and recommends creating the enrollment CNAME for each domain used for sign-in. See Microsoft's guidance on Windows enrollment in Intune at Set up enrollment for Windows devices and the CNAME validation guidance at Create CNAME DNS records for simplified Windows enrollment.

QUESTION NO: 18

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 correct because Windows includes policy settings under Local Group Policy that can disable access to the Microsoft Store app. On workgroup computers, these settings can be configured locally by using the Local Group Policy Editor, so domain Group Policy is not required. The relevant policy is commonly found under Windows Components\Store and can be used to turn off the Store application. Microsoft documents Microsoft Store access management for Windows clients in Configure access to Microsoft Store.

From Security Settings in the local Group Policy, configure Application Control Policies is also correct because Application Control Policies include AppLocker. AppLocker supports packaged app rules, which can be used to control Microsoft Store apps and packaged app installers for specific users or groups. This makes it a valid local policy-based method to prevent users from launching Store apps on Windows 10 computers that are not joined to a domain. Microsoft describes AppLocker support for packaged apps in Packaged apps and packaged app installers in AppLocker.

QUESTION NO: 19

You have 25 computers that run Windows 10 Pro.

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

You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.

What should you use?

A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise

B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise

C. Windows Autopilot

D. Subscription Activation

E. A feature update policy in Microsoft Intune

ANSWER: E

Explanation:

A feature update policy in Microsoft Intune is the best fit because it uses Windows Update for Business to perform an in-place feature upgrade from Windows 10 to Windows 11 while preserving user data, apps, and settings. In Intune, you can create a Feature updates for Windows 10 and later policy, select the target Windows 11 release, and assign it to the 25 managed devices. This minimizes administrative effort because it avoids building images, creating deployment task sequences, or manually running setup on each computer. Microsoft documents that Intune feature update policies can be used to keep devices on a specific Windows feature version and to upgrade eligible Windows 10 devices to Windows 11. With Microsoft 365 E5 licensing, the devices also have the Windows Enterprise entitlement; after the OS upgrade, Enterprise subscription activation can apply based on the assigned user license. See Microsoft's guidance for feature updates in Intune and Windows subscription activation.

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 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 corporate-owned Android Enterprise fully managed devices, Intune deploys public Android apps through the managed Google Play integration. To make App1 available for assignment in Intune, you first need to use the Managed Google Play Store to approve App1. Approval adds the app to the organization's managed Google Play collection and allows Intune to manage it for enrolled Android Enterprise devices. After the app is approved, you must sync App1 with Intune so that the

approved app is imported into the Microsoft Intune admin center and becomes available as an app object that can be assigned to device or user groups.

This workflow is the standard preparation process for deploying managed Google Play apps to Android Enterprise devices, including fully managed devices. Microsoft documents that admins select and approve apps from managed Google Play, then synchronize them so they appear in Intune for deployment and policy management. See Microsoft's guidance for adding managed Google Play apps in Intune: Add managed Google Play apps to Android Enterprise devices with Intune and Assign apps to groups with Microsoft Intune.

QUESTION NO: 21

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.

You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following requirements:

Ensure that any applications installed by the users are retained. Minimize user intervention.

What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Windows Autopilot

B. Microsoft Deployment Toolkit (MDT)

C. a Windows Configuration Designer provisioning package

D. Windows Deployment Services (WDS)

ANSWER: C

Explanation:

A Windows Configuration Designer provisioning package is the best fit because it applies configuration to an existing Windows installation instead of replacing the operating system image. That is important here because the users already own Windows 10 Pro devices and any applications they installed must be retained. A provisioning package can be created to perform common runtime provisioning tasks, including joining the device to Azure AD, applying configuration settings, adding apps, and performing an edition upgrade when the required licensing or product key configuration is supplied. The user experience can be very lightweight: the package can be delivered as a file or on removable media, and applying it can automate multiple setup steps without requiring a full deployment process or device wipe. Microsoft describes provisioning packages as a way to quickly configure Windows devices without imaging, and Windows edition upgrade documentation identifies supported methods for moving from Windows Pro to Enterprise. See Provisioning packages for Windows and Windows edition upgrades.

QUESTION NO: 22

You are creating a device configuration profile in Microsoft Intune.

You need to configure specific OMA-URI settings in the profile.

Which profile type template should you use?

A. Device restrictions (Windows 10 Team)

B. Identity protection

C. Custom

D. Device restrictions

ANSWER: C

Explanation:

Custom

is correct because Microsoft Intune uses custom device configuration profiles when you need to deploy settings by specifying Open Mobile Alliance Uniform Resource Identifier (OMA-URI) values directly. A custom profile lets an administrator define each setting with a name, description, OMA-URI path, data type, and value. This is the appropriate profile type when the required configuration is not available as a built-in Intune settings catalog or template setting, or when documentation from Microsoft or another vendor provides a specific Configuration Service Provider (CSP) OMA-URI that must be configured manually.

For Windows devices, Intune custom profiles are commonly used to configure CSP-based policies by entering the OMA-URI and value that correspond to the desired Windows policy setting. Microsoft's Intune documentation specifically describes creating a custom profile and adding OMA-URI settings for Windows client devices. The Windows CSP documentation also provides the OMA-URI paths that Intune can use for supported policy areas. See Use custom settings for Windows devices in Microsoft Intune and Configuration service provider reference.

QUESTION NO: 23

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:

To allow User1 to start a Remote Help session for Device1 from the Intune admin center, the Remote Help client must be available on the target device, User1 must have the appropriate Intune RBAC permissions, and User1 must be licensed for the Remote Help capability. Deploy the Remote Help app to Device1 is correct because Remote Help requires the app on the device that will participate in the assistance session. Assign the Help Desk Operator role to User1 is correct because Microsoft's built-in Help Desk Operator role includes the Remote Help permissions needed to view the screen or take control, subject to scope and assignment. Assign the Remote Help add-on license to User1 is also correct because helpers must be licensed for Remote Help; this entitlement can be provided through the standalone Remote Help add-on or through Microsoft Intune Suite licensing. Microsoft documents these requirements in the Remote Help prerequisites and RBAC guidance for Intune. See Remote Help with Microsoft Intune and Remote Help on Windows.

QUESTION NO: 24

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:

To deliver Windows 11 devices directly to users and have them configured during the out-of-box experience, you should use automatic enrollment together with a Windows Autopilot deployment profile for user-driven mode. Automatic enrollment enables supported Microsoft Entra ID users to have their devices automatically enrolled into Microsoft Intune when the device joins or registers with Microsoft Entra ID. This is the Intune enrollment component that ensures the device becomes managed after the user signs in with organizational credentials. Microsoft documents this capability as automatic MDM enrollment for Microsoft Entra joined devices: Enroll Windows devices in Intune.

A Windows Autopilot deployment profile for user-driven mode is the correct Autopilot configuration because the scenario specifically requires users to be prompted to sign in during OOBE. User-driven mode is designed for devices shipped directly to users; during setup, the user authenticates with their work or school account, and Autopilot applies the assigned deployment profile and enrollment settings. Microsoft describes user-driven Autopilot as the standard approach for new Windows devices where users complete OOBE and the device is enrolled and configured through Intune: Windows Autopilot user-driven mode.

QUESTION NO: 25

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 is correct because Intune can deploy the Windows Policy CSP setting **System/AllowBuildPreview** by using a custom OMA-URI. Setting this policy to disable build preview access prevents users from controlling Windows Insider Preview build enrollment from the Windows settings experience. Microsoft documents this CSP as the policy that controls user access to Insider Preview build settings, so it directly satisfies the requirement to stop users from enrolling devices in the Windows Insider Program. See Policy CSP - System/AllowBuildPreview.

A Windows 10 and later update ring is also correct because Intune update rings manage Windows Update for Business settings, including pre-release or Windows Insider build behavior. By configuring the Insider/pre-release build setting so that pre-release builds are disabled or not allowed, administrators can centrally prevent assigned Windows 10 devices from being moved to Insider channels. Update rings are designed for this type of Windows servicing control and can be assigned to device groups from the Intune admin center. See Windows update settings in Intune.

QUESTION NO: 26

You use a Microsoft Intune subscription to manage iOS devices.

You configure a device compliance policy that blocks jailbroken iOS devices.

You need to enable Enhanced jailbreak detection.

What should you configure?

A. the Compliance policy settings

B. the device compliance policy

C. a network location

D. a configuration profile

ANSWER: A

Explanation:

the Compliance policy settings is correct because Enhanced jailbreak detection is configured as an Intune compliance policy setting, not as an individual iOS/iPadOS compliance policy rule. In Intune, the per-platform compliance policy can include a rule to mark jailbroken devices as noncompliant, but the Enhanced jailbreak detection feature is enabled from the tenant-level compliance policy settings area. This setting changes how Intune performs jailbreak detection for enrolled iOS/iPadOS devices, providing additional jailbreak checks beyond the standard compliance evaluation. Microsoft documents this under compliance policy settings, where administrators can configure settings that affect how device compliance is evaluated across the Intune tenant. After Enhanced jailbreak detection is enabled, devices identified as jailbroken can be marked noncompliant and then acted on by compliance actions or Conditional Access policies. For more detail, see Microsoft's documentation for device compliance policies in Intune and iOS/iPadOS compliance settings.

QUESTION NO: 27

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 correct because the folder is being accessed through a shared folder, so both the share permissions and the NTFS permissions are evaluated together. The effective access over the network is limited by the more restrictive result of those two permission layers. In this case, the NTFS permissions grant Full control to Everyone, so NTFS does not further restrict either user. The deciding factor is the share permission assigned to each user. A user with Full Control share permission can perform all Change-level file operations and can also perform administrative security actions through the share, including changing permissions and taking ownership. A user with only Change share permission can modify content, but does not receive those Full Control-only security capabilities through the share. Therefore, when User1 has Full Control at the share level and User2 has Change at the share level, User1 can set file permissions and take ownership of files in Share1, while User2 cannot. See Microsoft's guidance on how share and NTFS permissions combine in Share and NTFS Permissions on a File Server and the SMB share access rights described for Grant-SmbShareAccess.

QUESTION NO: 28

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM). You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.

What should you do?

A. From the Microsoft Intune admin center, create a Windows 10 device profile.

B. From Azure AD, add an app registration.

C. From Azure AD, add an enterprise application.

D. From the Microsoft Intune admin center, add an app.

ANSWER: D

Explanation:

From the Microsoft Intune admin center, add an app.
is correct because Microsoft Intune provides a dedicated app type for deploying Microsoft 365 Apps to managed Windows devices. For Windows 10 devices enrolled in MDM, you deploy the suite by going to Apps in the Intune admin center, adding a new app, and selecting the Microsoft 365 Apps app type for Windows 10 and later. This deployment method lets you choose the Office apps to install, configure update channels, architecture, version settings, and assign the app to users or device groups. Once assigned, Intune delivers the Microsoft 365 Apps for enterprise installation to the enrolled computers according to the assignment intent, such as Required. This is the supported management path for deploying Office apps through cloud-based endpoint management rather than using device configuration profiles or Microsoft Entra application objects. Microsoft documents this workflow in its guidance for adding Microsoft 365 Apps to Windows devices in Intune and assigning apps to users or devices. See Add Microsoft 365 Apps to Windows devices with Microsoft Intune and Add apps to Microsoft Intune.

QUESTION NO: 29

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

You use Microsoft Intune to manage devices.

You need to review the startup times and restart frequencies of the devices.

What should you use?

A. Azure Monitor

B. Intune Data Warehouse

C. Microsoft Defender for Endpoint

D. Endpoint analytics

ANSWER: D

Explanation:

Endpoint analytics is the correct choice because it is the Intune feature designed to help endpoint administrators measure and improve the user experience on managed devices. Its reports include startup performance information, such as device boot time and sign-in time, which directly supports reviewing startup times across the organization. Endpoint analytics also surfaces device health and performance signals that help administrators identify devices that restart frequently or otherwise contribute to poor productivity experiences. These insights are available from the Microsoft Intune admin center and are intended specifically for monitoring and improving endpoint performance, rather than for general infrastructure monitoring or security investigation.

Microsoft describes Endpoint analytics as a set of reports that provides insights for measuring how the organization is working and for improving device performance and reliability. The startup performance report is specifically focused on helping identify devices with slow boot or sign-in experiences. For more information, see Endpoint analytics overview and Startup performance in Endpoint analytics.

QUESTION NO: 30

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 correct because these Microsoft Intune app information fields are intended to be surfaced to users in the Company Portal. When you add an app in the Microsoft Intune admin center, the app information page includes metadata that helps users identify the app and learn more before installing it. Microsoft's Intune app configuration guidance states that the Information URL is an optional website link containing more information about the app,

and that this URL is displayed in the Company Portal. It also states that the Privacy URL is an optional website link containing privacy information for the app, and that this URL is displayed in the Company Portal. These fields are user-facing app details, so they are appropriate for an app catalog experience where users browse and install available apps. See Microsoft's app information field descriptions in the Intune app management documentation: Add apps to Microsoft Intune and the Microsoft Store app deployment guidance: Add Microsoft Store apps to Microsoft Intune.

QUESTION NO: 31

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

A. 1 only

B. 2 and 3 only

C. 1 and 3 only

D. 1, 2, and 4 on

E. 1, 2, 3, and 4

ANSWER: D

Explanation:

The choice that includes events 1, 2, and 4 is correct because the Windows event log collection settings for a Log Analytics workspace collect the supported Windows event types selected in the workspace configuration. When all available Windows event log event types are selected for the legacy Log Analytics agent, the supported event types are collected from the configured logs, such as Error, Warning, and Information events. This matches the events identified as 1, 2, and 4 in the table. In this configuration, Log Analytics is not simply ingesting every possible Windows Event Viewer record without regard to the event type or collection mechanism; it ingests the Windows event categories supported by that data source. Microsoft documents Windows event log collection for the Log Analytics agent as a data source where you specify event logs and event types to collect. Security audit event collection is handled through dedicated security event collection mechanisms rather than by assuming every Windows event category is included just because Windows event logs are enabled. See Microsoft's documentation for Windows event log data sources in Azure Monitor.

QUESTION NO: 32

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.

Which extension should you select for the app package file?

A. .intunemac

B. apk

C. jpa

D. .appx

E. .ipa

ANSWER: E

Explanation:

.ipa is correct because Microsoft Intune requires iOS/iPadOS line-of-business app packages to be uploaded as iOS application archive files. An .ipa file is the standard packaged format for apps built for iPhone and iPad, and it contains the compiled app bundle and required metadata for installation on Apple devices. In Intune, when you add an iOS/iPadOS line-of-business app, the app package file type must be an .ipa file before Intune can deploy it to enrolled iOS/iPadOS devices. This deployment method is intended for custom apps that are developed internally or obtained outside the public App Store, typically signed with an appropriate Apple certificate or provisioning profile so managed devices can install and run the app. Microsoft's Intune app deployment documentation identifies iOS/iPadOS LOB apps as using an .ipa installation file. You can confirm this in the Microsoft Learn guidance for adding apps to Intune and the specific article for adding iOS/iPadOS line-of-business apps: Add apps to Microsoft Intune and Add an iOS/iPadOS line-of-business app to Microsoft Intune.

QUESTION NO: 33

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:

Log Analytics can collect several common data types from Windows client computers through Azure Monitor data sources. "error events from the System log" is correct because Windows event log collection supports collecting events from standard Windows logs, including the System log, based on selected event levels such as Error, Warning, and Information. "third-party application logs stored as text files" is also correct because custom log collection can ingest text-based log files created by applications, allowing those records to be queried in a Log Analytics workspace. "the average processor utilization

" is correct because performance counters can be collected from Windows computers, including processor counters such as Processor\% Processor Time, which can be queried and averaged in Log Analytics. These capabilities align with the Azure Monitor/Log Analytics agent data source model, where event logs, custom logs, and performance counters are standard supported collection sources. See Microsoft's documentation for Log Analytics agent data sources at Azure Monitor agent data sources and custom log collection at Collect custom logs with Log Analytics agent.

QUESTION NO: 34

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

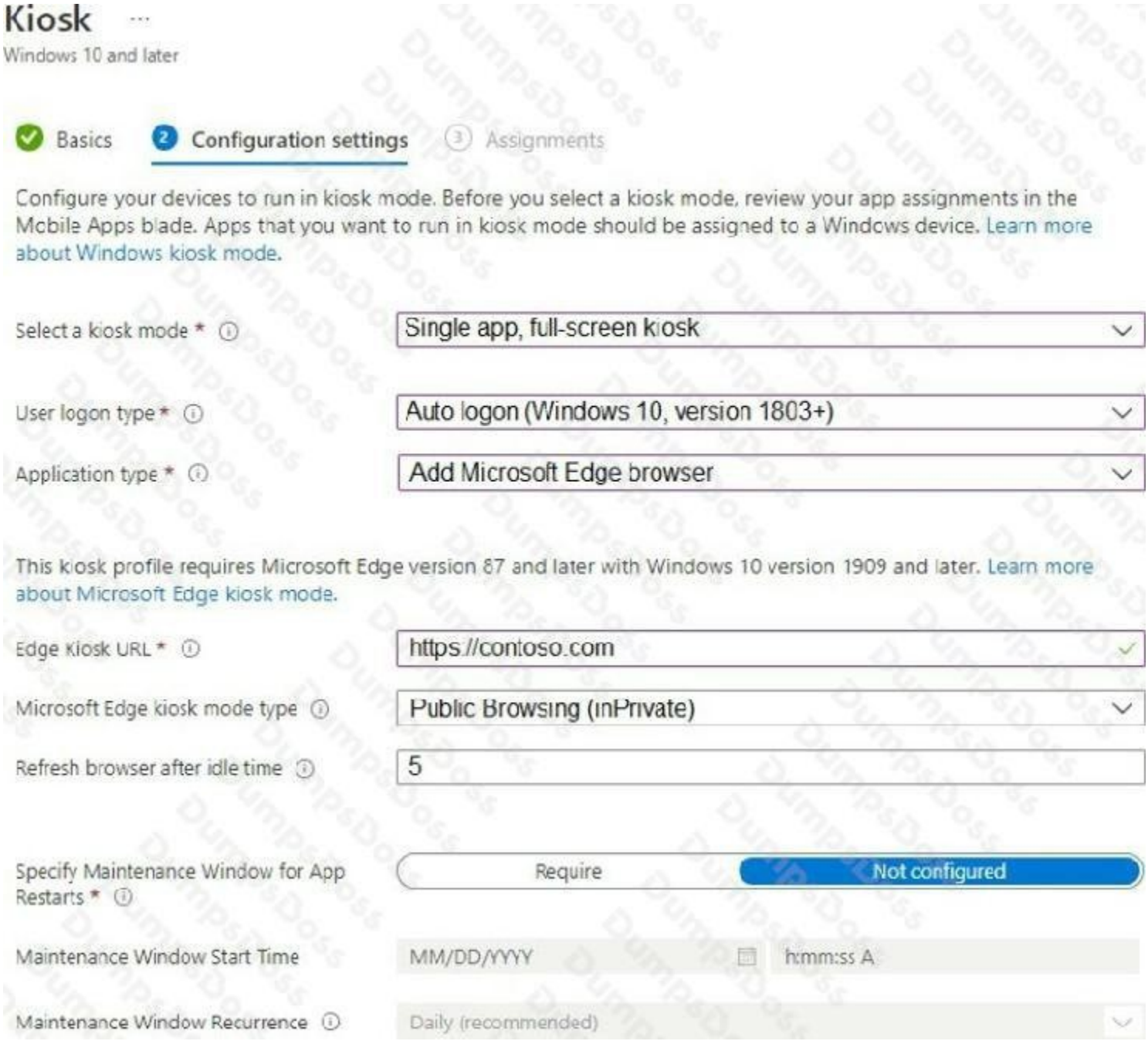
Explanation:

To allow User1 to start and use Remote Help for Device1 from the Intune admin center, User1 and the target device must meet the Remote Help prerequisites. Deploy the Remote Help app to Device1 is required because Remote Help sessions rely on the Remote Help client being available on the managed endpoint. Assign the Help Desk Operator role to User1 is appropriate because Remote Help is controlled through Intune role-based access control, and support personnel need a role that grants the required remote assistance permissions. Assign the Remote Help add-on license to User1 is also required because Remote Help is a separately licensed Intune capability; when an organization has Microsoft Intune Suite or the Remote Help add-on, eligible users still need the license entitlement assigned so they can act as helpers. Microsoft documents Remote Help licensing, app installation, and RBAC requirements in the Intune Remote Help guidance. See Use Remote Help with Microsoft Intune and Role-based access control with Microsoft Intune.

QUESTION NO: 35 - (HOTSPOT)

HOTSPOT -

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

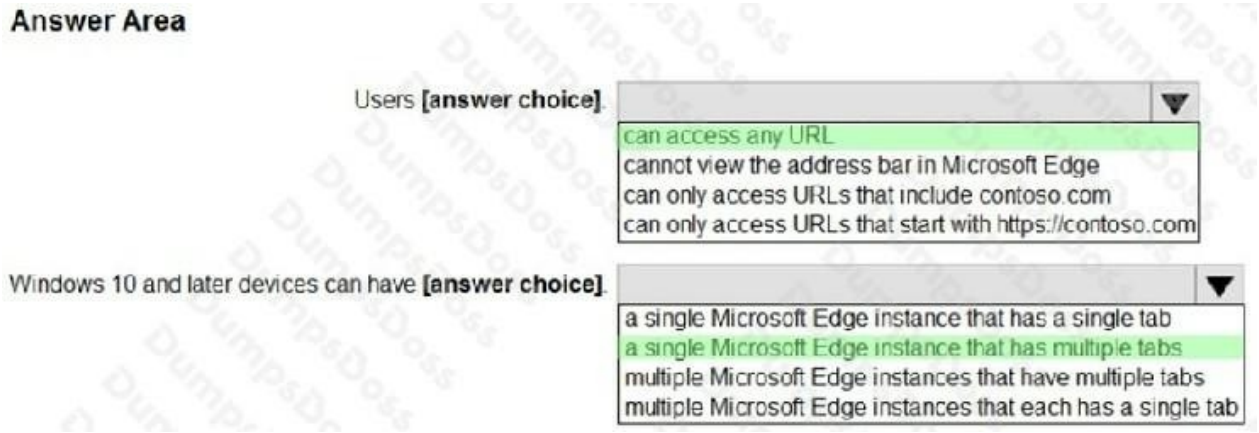
Users **[answer choice]**.

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have **[answer choice]**.

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

ANSWER:



Explanation:

The correct selections are that users can access any URL and that Windows 10 and later devices can have a single Microsoft Edge instance that has multiple tabs. In a Microsoft Edge kiosk configuration that uses the public browsing experience, the URL configured in the profile acts as the page that Edge opens to, but it is not automatically treated as an allow-list restriction. Unless additional URL filtering policies are configured, users are still able to browse away from the configured start page and enter other addresses. That is why the user-facing result is that users can access any URL rather than being limited to only URLs that contain or begin with the Contoso address.

The second selection follows from how Microsoft Edge kiosk mode behaves in public browsing mode. Public browsing is intended for shared or public-use devices where the browser runs in a managed, limited experience. Microsoft describes this mode as a multi-tab browsing experience, while still running as a controlled kiosk browser session. That matches the statement that Windows 10 and later devices can have a single Microsoft Edge instance that has multiple tabs. This is the key distinction: the kiosk profile controls the Edge session, but the public browsing mode still supports multiple tabs inside that browser instance. For more detail, see Microsoft's documentation on configuring Microsoft Edge kiosk mode and the Intune documentation for Windows kiosk settings in Microsoft Intune.

QUESTION NO: 36

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:

Log Analytics can collect the average processor utilization because Windows performance counters are a supported data source for Azure Monitor/Log Analytics. Processor counters such as percentage processor time can be sampled and sent to the workspace, where they are stored for querying and alerting. Log Analytics can also collect error events from the System log because Windows event logs are a standard supported source; administrators can configure collection rules to gather selected event levels from logs such as System and Application. Third-party application logs stored as text files are also supported through custom or text log collection, allowing line-based log files on monitored Windows computers to be

ingested into a Log Analytics workspace for analysis. These capabilities align with Microsoft's documented Azure Monitor data collection model, which supports Windows event logs, performance counters, and text-based logs from monitored machines. See Microsoft's guidance for collecting Windows events and collecting text logs.

QUESTION NO: 37

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 Azure AD joined Windows 10 devices that are already managed by Microsoft Intune, the lowest-effort administrative approach is to manage both Microsoft Defender Antivirus and Microsoft Defender Firewall directly from Intune by using a device configuration profile with Endpoint protection settings. "To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings" is correct because Intune Endpoint protection profiles include Microsoft Defender Antivirus configuration settings that can be assigned centrally to device groups. "To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings" is also correct because the same Intune profile area supports Microsoft Defender Firewall configuration, allowing firewall behavior and related protection settings to be applied consistently across managed Windows devices. This aligns with Microsoft's Intune management model for cloud-joined endpoints: policies are created in the Intune admin center and deployed to enrolled devices without requiring on-premises domain infrastructure or local configuration on each device. Microsoft documents Windows device configuration profiles and Endpoint protection settings for managing Defender technologies through Intune. See Create device profiles in Microsoft Intune and Endpoint protection settings for Windows in Intune.

QUESTION NO: 38

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: B

Explanation:

Microsoft Secure Score is the correct tool to use when you need to evaluate your current security configuration against Microsoft-recommended practices. Secure Score measures an organization's security posture and provides recommended actions that show where your environment differs from Microsoft's recommended configuration baseline. For Microsoft Defender for Endpoint, Secure Score can surface endpoint-related improvement actions and help administrators prioritize changes that improve protection for Windows devices. The score is not just a reporting dashboard; it is designed to provide actionable guidance, tracking, and visibility into configuration gaps across Microsoft security workloads, including endpoint security. Microsoft documents Secure Score as a way to assess security posture and follow recommended actions to improve protection over time. See Microsoft Secure Score and Microsoft Secure Score for Devices.

QUESTION NO: 39

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

10.

You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

A. Group2 only

B. Group1 and Group2 only

C. Group2 and Group3 only

D. Group1, Group2, and Group3

ANSWER: A

Explanation:

Group2 only is correct because Group4 is a global group, and Active Directory group nesting rules are restrictive for global groups. A global group can contain user accounts, computer accounts, and other global groups, but only from the same domain. In this scenario, Group2 is the only group that matches the required membership rule for being added to Group4. This is the standard Active Directory group scope behavior used for role-based access design: global groups are intended to collect accounts or other global groups from the same domain, and then those global groups can be assigned access indirectly through domain local groups or local groups as needed.

Microsoft documents that global groups can include accounts and global groups from the same domain, while their permissions can be assigned in any domain in the forest or trusting domains. This same-domain nesting limitation is what

determines the valid choice here. For more detail, see Microsoft's guidance on Active Directory security groups and security group nesting.

QUESTION NO: 40

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: B D

Explanation:

To ensure that only Android devices using Android work profiles can enroll in Intune, you must allow enrollment for the Android Enterprise work profile platform and block enrollment through the legacy Android device administrator platform. The configuration "From Platform Settings, set Android Enterprise (work profile) to Allow" enables personally owned Android Enterprise work profile enrollment, which creates a separate managed work profile on the device for corporate apps and data. The configuration "From Platform Settings, set Android device administrator to Block" prevents Android devices from enrolling by using the older device administrator management method, ensuring that Android enrollment is limited to the work profile experience. Microsoft's Intune enrollment restrictions let administrators control which platforms and enrollment types are allowed or blocked, including Android Enterprise work profile and Android device administrator enrollment. This aligns with Microsoft's recommended direction for Android management, where Android Enterprise work profiles are used to manage corporate data on personal Android devices while maintaining separation from personal data. For more information, see Set enrollment restrictions in Microsoft Intune and Enroll Android Enterprise personally owned devices with a work profile.

QUESTION NO: 41

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com. Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A. Yes

B.

No

ANSWER: B

Explanation:

No is correct because changing Microsoft Entra user settings and device settings does not configure Windows Hello for Business PIN complexity. Those Entra settings can affect device join, registration, and whether Windows Hello for Business is enabled or used during sign-in, but the required PIN length is controlled through Windows Hello for Business policy settings. To require a six-digit PIN, an administrator must configure the PIN complexity policy, such as the minimum PIN length, by using Microsoft Intune account protection or device configuration settings, or by using the Windows Hello for Business policy settings backed by the PassportForWork configuration service provider. Microsoft documents the Windows Hello for Business PIN complexity controls, including minimum PIN length, as configurable policy settings rather than general Entra tenant user or device settings. In this scenario, the stated solution would leave the default four-digit PIN behavior unchanged, so users would not reliably be prompted to create a six-digit PIN when joining Windows 10 devices to the tenant. See Microsoft's Windows Hello for Business Intune settings and the PassportForWork CSP reference for the relevant minimum PIN length configuration: Windows Hello for Business settings in Intune and PassportForWork CSP.

QUESTION NO: 42

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: D E

Explanation:

For Intune-managed Windows 10 devices that are Azure AD joined, the lowest-effort approach is to configure the required Defender settings directly through Intune device configuration profiles. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings is correct because the Windows 10/11 device restrictions profile includes a Microsoft Defender Antivirus section for common antivirus controls such as real-time monitoring, cloud-delivered protection, sample submission behavior, scanning options, and exclusions. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings is correct because the Endpoint protection profile contains the Microsoft Defender Firewall configuration areas for domain, private, and public firewall profiles and related firewall behavior. This aligns with managing cloud-joined devices through Intune rather than using on-premises Group Policy, which would add unnecessary infrastructure and administration for Azure AD joined,

Intune-managed endpoints. See Microsoft's Intune documentation for Windows device restrictions settings and Windows endpoint protection settings.

QUESTION NO: 43

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments.

From Deployment Workbench, you modify the WinPE settings and add PowerShell support.

You need to generate a new set of WinPE boot image files that contain the updated settings.

What should you do?

A. From the Deployment Shares node, update the deployment share.

B. From the Advanced Configuration node, create new media.

C. From the Packages node, import a new operating system package.

D. From the Operating Systems node, import a new operating system.

ANSWER: A

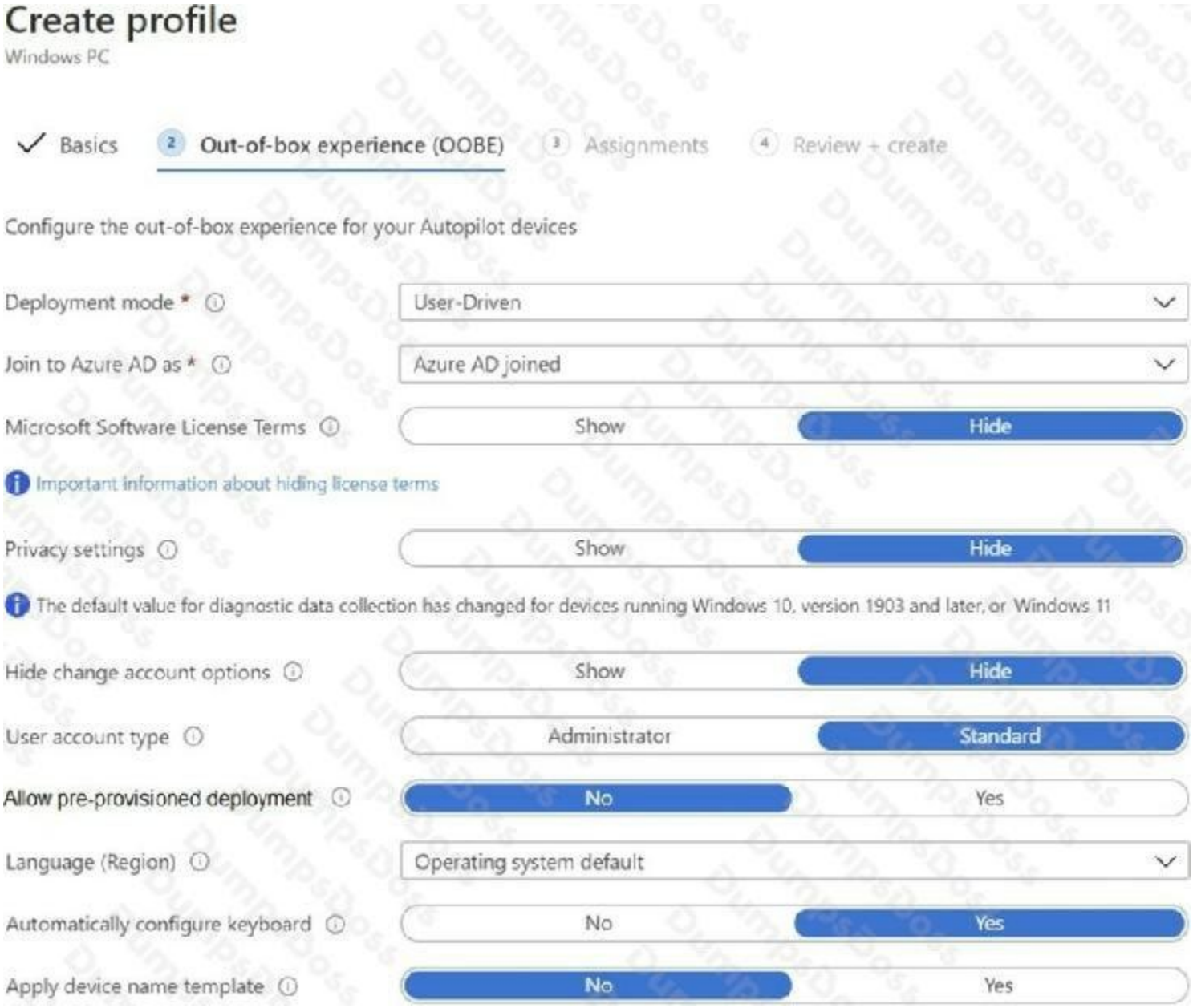
Explanation:

From the Deployment Shares node, update the deployment share is correct because MDT stores the Windows PE configuration for a deployment share and uses that configuration when it regenerates the Lite Touch boot images. After changing Windows PE settings in Deployment Workbench, such as enabling PowerShell support, you must run the Update Deployment Share action so MDT can rebuild the boot image files, including the updated optional components and settings. This process creates or refreshes the bootable LiteTouchPE images, such as the WIM and ISO files, under the deployment share's Boot folder. If the goal is to make the updated WinPE configuration available for PXE boot, removable media, or ISO-based booting, updating the deployment share is the required step. Microsoft's MDT documentation describes the deployment share update process as the action that creates the boot images used to start the deployment environment. For more information, see Microsoft's guidance on creating and updating MDT deployment shares and the MDT deployment preparation workflow.

QUESTION NO: 44 - (HOTSPOT)

HOTSPOT -

You have a Microsoft Intune subscription.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

Users who deploy a device by using Profile1 **[answer choice].**

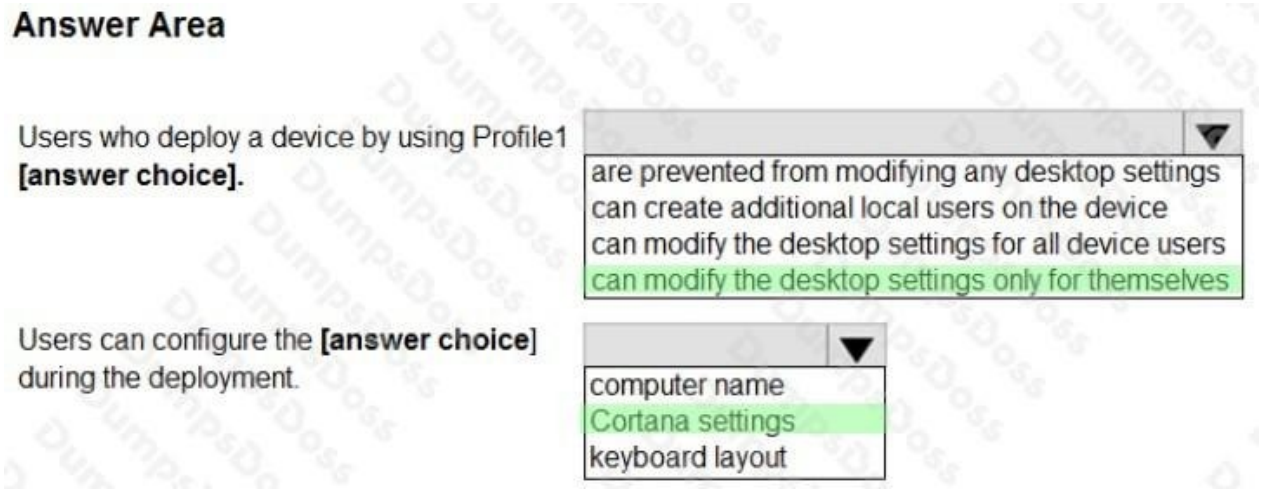
- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment.

- computer name
- Cortana settings
- keyboard layout

NOTE: Each correct selection is worth one point.

ANSWER:



Explanation:

The selected answers are correct because the Windows Autopilot deployment profile controls both the account privileges assigned to the user during enrollment and which out-of-box experience screens remain available. In the profile, the user account type is configured as a standard user. A standard user can personalize their own Windows experience, including user-specific desktop settings, but does not receive local administrator permissions for device-wide configuration. That makes “can modify the desktop settings only for themselves” the correct completion for the first statement. This matches how Windows separates per-user settings from administrative, device-level changes through User Account Control and standard user permissions. Microsoft describes the distinction between standard and administrator behavior in Windows in its documentation for User Account Control.

The second selected answer is also correct because the Autopilot profile settings determine which OOBE pages are skipped or shown during Windows 10 deployment. Since the profile does not suppress the Cortana-related OOBE experience for Windows 10, the user can configure Cortana settings during the deployment process. Autopilot deployment profiles are specifically designed to customize the OOBE flow, including hiding or showing selected setup pages and defining the user account type used after enrollment. Microsoft documents these configurable profile behaviors in Windows Autopilot deployment profiles. So, with the user account type set to standard and the Windows 10 OOBE flow allowing Cortana configuration, the selected statements accurately reflect what the user can do during and after deployment with Profile1.

QUESTION NO: 45

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to deploy a custom app to Android devices. The app uses the APK file format.

Which type of app should you select for the deployment?

A. built-in

B. Android store

C. Managed Google Play

D. line-of-business (LOB)

E. web link

ANSWER: D

Explanation:

line-of-business (LOB) is correct because Microsoft Intune supports deploying custom Android applications packaged as APK files by adding them as Android line-of-business apps. A line-of-business app is intended for internally developed or privately distributed apps that are not being deployed as a standard public store app. In the Intune admin center, this app

type allows an administrator to upload the APK package, configure app information, and assign the app to users or device groups for deployment. This matches the scenario exactly: the organization has a custom Android app, and the provided installation package is in APK format.

Microsoft's Intune documentation specifically describes adding an Android line-of-business app and notes that this app type is used to upload an APK app package file. For current Android Enterprise scenarios, Microsoft also provides guidance around managed Google Play private apps, but when the exam question explicitly states that you need to deploy a custom app using an APK file format, the Intune app type that directly corresponds to uploading that package is line-of-business. See Microsoft's guidance on adding Android line-of-business apps to Microsoft Intune and the broader Intune app type documentation.

QUESTION NO: 46

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:

To enable Windows Remote Management centrally on domain-joined Windows 10 computers by using Group Policy, you need to configure the WinRM service, allow WinRM listener configuration, and permit the required inbound management traffic. Setting the Startup Type of the Windows Remote Management (WS-Management) service to Automatic ensures the WinRM service starts reliably on each managed computer without requiring a manual command such as winrm quickconfig. Enabling the Allow remote server management through WinRM setting configures the WinRM service to listen for remote management requests, typically by defining the IPv4 and/or IPv6 listener filters that identify which remote sources are allowed. Enabling the Windows Firewall: Allow inbound remote administration exception setting allows the remote management traffic required for administrators to connect to and manage the computers remotely. Together, these Group Policy settings provide the service state, listener configuration, and firewall access needed for WinRM-based remote administration at scale. Microsoft documents WinRM as the Windows implementation of WS-Management and describes Group Policy-based configuration for the WinRM service and firewall requirements in its WinRM guidance: Windows Remote Management and Installation and configuration for Windows Remote Management.

QUESTION NO: 47

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 and Enroll the devices in Microsoft Intune by using Apple Business Manager are correct. To control iOS/iPadOS software update behavior in Intune, the iPad devices must be managed and supervised. Apple Business Manager with Automated Device Enrollment is the standard scalable method for enrolling corporate-owned Apple devices into Intune as supervised devices, which enables stronger management controls than user-driven Company Portal enrollment alone. Once the devices are supervised and enrolled, Intune can apply configuration settings that manage software update behavior, including deferring update visibility and controlling when updates are available or installed. This is what prevents users from manually installing a newer iOS/iPadOS version before the organization allows it. Microsoft documents that Apple automated device enrollment supports supervised management through Intune, and that Intune can manage iOS/iPadOS software updates for supervised devices. See Automatically enroll iOS/iPadOS devices with Apple Business Manager and Manage iOS/iPadOS software update policies in Intune.

QUESTION NO: 48

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

A. Session access controls

B. an assignment that uses a User risk condition

C. an assignment that uses a Sign-in risk condition

D. Grant access controls

ANSWER: A

Explanation:

Session access controls is correct because Conditional Access uses session controls to manage what happens after access is granted, including how often users must reauthenticate. To require members of Group1 to reauthenticate every eight hours when accessing Microsoft Exchange Online, you configure the Conditional Access policy's session setting for sign-in frequency and set the interval to 8 hours. Sign-in frequency defines the period before a user is prompted to sign in again when the policy applies to the selected users or groups and cloud apps.

In this scenario, CAPolicy1 is already assigned to Group1, and the target cloud app would be Microsoft Exchange Online. The required behavior is not about blocking access or requiring MFA at initial sign-in only; it is specifically about controlling the lifetime of the authenticated session. Microsoft documents sign-in frequency as a Conditional Access session control that can be configured in hours or days. For more information, see Microsoft Learn: Session controls in Conditional Access and Configure authentication session management.

QUESTION NO: 49

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

You need to enable self-service password reset on the sign-in screen.

Which settings should you configure from the Microsoft Intune admin center?

A. Device configuration

B. Device enrollment

C. Conditional access

D. Device compliance

ANSWER: A

Explanation:

Device configuration is correct because enabling self-service password reset from the Windows sign-in screen is a device policy setting that can be deployed to managed Windows devices through Intune. For Azure AD-joined Windows 10 devices enrolled in Microsoft Intune, administrators can create a Windows device configuration profile, such as a Settings catalog profile or custom policy, to configure the policy that allows users to reset their Azure AD password directly from the lock/sign-in screen. This capability is controlled on the device, so it belongs in the Intune device configuration area rather than user access evaluation or enrollment workflows. Microsoft documents the relevant Windows policy setting as **AllowAadPasswordReset**, which enables the “Reset password” link on the Windows sign-in screen for supported Azure AD-joined devices. Intune is the management plane used to push that configuration consistently to all enrolled Windows 10 computers. See Microsoft’s documentation for the Policy CSP authentication setting at Policy CSP - Authentication and Intune device configuration profiles at Create device profiles in Microsoft Intune.

QUESTION NO: 50

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 correct because Intune app protection policies are designed to control how corporate data is handled inside managed apps, including Microsoft 365 apps on iOS/iPadOS. These policies apply data loss prevention controls at the app level, so they can restrict actions such as moving organizational data to unmanaged apps, saving copies to personal storage locations, and printing organizational data. For this scenario, the relevant Intune app protection policy setting is the iOS/iPadOS data protection control for “Printing Org data,” which can be configured to block users from printing corporate data from apps protected by Intune.

This is especially appropriate when the requirement is specifically about “managed apps” rather than device-wide configuration. App protection policies can protect corporate data whether devices are enrolled in Intune or used in certain unmanaged/BYOD scenarios, as long as the apps support Intune app protection. Microsoft documents these controls under Intune app protection policy data protection settings for iOS/iPadOS and explains that app protection policies help safeguard

organization data at the app layer. See Microsoft Intune app protection policies and iOS/iPadOS app protection policy settings.