Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

MD-102 MCQs
MD-102 Exam Questions
MD-102 Practice Test
MD-102 TestPrep
MD-102 Study Guide

killexams.com

Microsoft

MD-102

Microsoft 365 Certified: Endpoint Administrator Associate

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/MD-102

Question: 1220

AVD multi-session Win10 22H2 needs custom RDP registry for USB redirection optimization. Target pool: (deviceOSType -eq "Windows") AND (osVersion -startswith "10.0.19045"). OMA-URI?

A. Use ADMX Terminal Server/TSUSBDevice policy Enabled

B. Custom profile HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\TSUSB

C. ./Device/Vendor/MSFT/Policy/Config/RDP/USBRedirectionOptimized with 1

Answer: B

Explanation: Custom OMA-URI targets specific RDP USB redirection registry for multi-session optimization unavailable in standard Settings catalog, ensuring AVD host performance.

Question: 1221

Transition 200 hybrid joined devices to Microsoft Entra joined for full cloud management. Minimize disruption, retain user profiles via Known Folder Move, and ensure Intune enrollment post-transition. Which steps are essential? (Choose three.)

A. Before disjoin, migrate profiles using tools preserving OneDrive-synced data

B. Run dsregcmd /leave then /join without reset

C. Use Autopilot reset to wipe and re-provision as Microsoft Entra joined

D. Keep hybrid join and adjust co-management sliders

E. Configure Intune MDM user scope to All for automatic enrollment after join

Answer: A,C,E

Explanation: Autopilot reset cleanly transitions to Microsoft Entra join by re-provisioning devices cloud-native. MDM user scope enables automatic Intune enrollment. Profile migration with OneDrive Known Folder Move preserves user data during the process.

Question: 1222

You are configuring a compliance policy for iOS/iPadOS. You need to ensure that devices are not "Jailbroken." Which setting should you enable?

A. Root access: Disable

B. System manipulation: Prevent

C. Jailbroken devices: Block

D. Device integrity: Secure

Answer: C

Explanation: In the iOS/iPadOS compliance policy under the "Device Health" section, the "Jailbroken devices" setting is specifically used to detect and block devices that have had their OS security layers bypassed.

Question: 1223

You are deploying a Windows Update Ring to a group of devices. You need to ensure that the "Automatic Update" behavior is set so that the user is notified to download the update, and once downloaded, they are notified to schedule a restart. Which two "Automatic update behavior" settings in Intune are applicable?

A. Notify install and restart

B. Scheduled install and restart

C. Auto install and restart at maintenance time

D. Auto install and notify install

E. Notify download

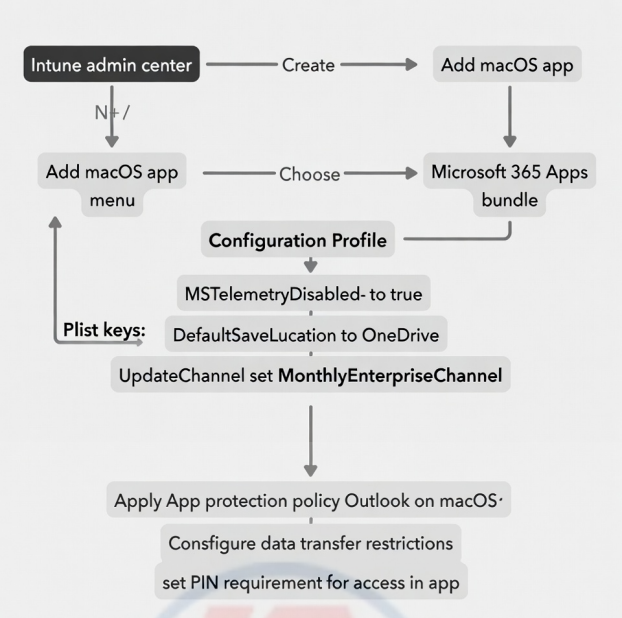
Answer: A,E

Explanation: "Notify download" ensures that the Windows Update agent does not consume bandwidth until the user acknowledges the update. Once the download is complete, "Notify install and restart" ensures the user remains in control of the actual installation and reboot process, which is often preferred for specialized workstations where an unexpected interruption could result in data loss or corrupted processes.

Question: 1224

Case study

Adventure Works uses Intune to manage macOS devices with Microsoft 365 Apps for Mac. They deploy Word, Excel, Teams via Intune macOS app type and need app configuration to disable telemetry, set default save to OneDrive, and configure update channel to Monthly Enterprise. They also plan app protection for Outlook on macOS personal devices.



How can telemetry be fully disabled for Microsoft 365 Apps on macOS?

A. Use Microsoft 365 Apps admin center privacy settings

B. Disable in app protection policy

C. Set com.microsoft.office.TelemetryLib.Enabled to false in configuration policy

D. Configure group policy preferences for macOS

Answer: C

Explanation: Disable telemetry comprehensively by creating a macOS app configuration policy for Microsoft 365 Apps and setting the preference key com.microsoft.office.TelemetryLib.Enabled to false, which prevents diagnostic data upload from the apps.

Question: 1225

New branch office deploys 100 laptops via Autopilot Entra join. Profile assignment delays due to dynamic group processing. You create static group first, upload HWIDs, wait 5min, then switch dynamic. Which cmdlet verifies profile assignment?

A. Get-MgDeviceManagementAutopilotDevice -Filter "serialNumber eq 'ABC123'"

B. Get-EntraDevice -Filter "displayName eq 'Laptop001'" | Select Profile

C. Get-AutopilotDiagnostics | Select ProfileStatus

D. dsregcmd /status | find "Profile"

Answer: A

Explanation: Get-MgDeviceManagementAutopilotDeviceIdentity -Filter "serialNumber eq 'ABC123'" (via Graph) retrieves assigned profile details post-HWID upload and group assignment, confirming Intune's periodic matching before physical deployment.

Question: 1226

Your organization uses Windows 365 with Intune Suite. You need to provision Cloud PCs with Microsoft Entra hybrid join support, apply Endpoint analytics insights for performance baselines, and scale sizes dynamically based on user location attribute.

Which three configurations are needed?

A. Provisioning policy with hybrid join type

B. Integrate Endpoint analytics to baseline Cloud PC performance

C. Dynamic groups using location attribute for size assignment

D. Custom gallery image with baseline scripts

E. Enable advanced analytics in Intune Suite

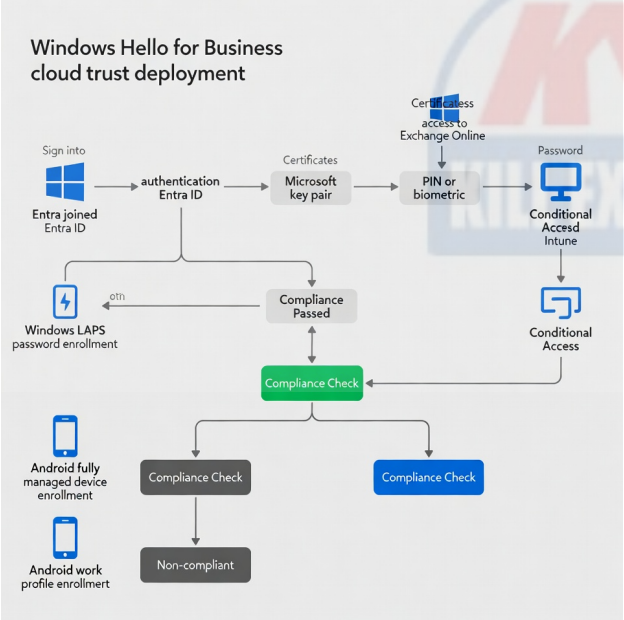
Answer: A,C,E

Explanation: Hybrid join provisioning policies support scenarios requiring on-premises resource access. Dynamic groups based on user attributes like location allow policy-based size scaling. Enabling Intune Suite advanced analytics provides performance baselines for Cloud PCs.

Question: 1227

Case study

Fabrikam operates in a highly regulated industry with 8,000 devices across Europe. They have Microsoft Entra ID P2 and Intune Suite. All Windows devices must use Windows Hello for Business cloud trust model with PIN and biometrics. Android devices use fully managed for corporate phones and work profile for BYO**D.** Compliance policies require jailbreak/root detection, minimum patch level, and encryption. Conditional Access requires compliant device status and excludes high-risk sign-ins. Windows LAPS is deployed with Entra ID backup and complex password requirements.



Which Conditional Access policy condition combination enforces compliance while allowing guest users limited access?

A. Target All cloud apps, require compliant device for All users including guests

B. Target Office 365 Exchange Online, require compliant device and sign-in risk low

C. Target All cloud apps, include All users and exclude Guests, require device compliance

D. Target All cloud apps, include All users, grant access only if compliant and exclude high-risk users

Answer: C

Explanation: Targeting All cloud apps, including All users but excluding Guests, and requiring device compliance ensures internal users must have compliant devices while allowing guest users access without device compliance checks.

Question: 1228

Your organization is implementing Microsoft Intune Remote Help for a global workforce. You must ensure that help desk technicians can only perform "Full Control" sessions on devices in the "Finance" group, while only being allowed "View Only" sessions for the "Executive" group. Which RBAC configuration strategy is required to achieve this granular control?

A. Use "Conditional Access App Control" in Microsoft Defender for Cloud Apps to intercept Remote Help sessions and downgrade permissions based on the device's "Management State" and "Group Membership".

B. Use the "Remote Help" app's internal "Access Control List" (ACL) to define "Group-to-Device" mappings and "Session Type" restrictions based on Entra ID attributes.

C. Create two custom roles: "Finance Remote Help" with "Take full control" permission and "Executive Remote Help" with "View screen" permission, then assign each to the technician group with different scope tags.

D. Modify the "Remote Help App" settings to include "Multiple Permission Levels" and map "Security Groups" to "Permission Tiers" within the Remote Help tenant settings.

Answer: C

Explanation: Microsoft Intune Remote Help permissions are governed by Intune Role-Based Access Control (RBAC). To differentiate session capabilities based on target device groups, you must define custom roles that specify the level of authority, such as "Take full control" versus "View screen". By utilizing Scope Tags, you can ensure that technicians assigned to these roles can only exercise those specific permissions when interacting with devices that share the corresponding Scope Tag, effectively isolating the "Full Control" capability to the Finance devices and "View Only" to the Executive devices.

Question: 1229

An organization uses Windows Autopilot self-deploying mode for kiosk devices in retail locations with no user affinity. The devices must be fully managed by Intune without on-premises AD access. Which join type and configuration steps are required? (Choose two)

A. Select Microsoft Entra joined in the Autopilot profile Join to Microsoft Entra ID as setting

B. Ensure the deployment profile uses user-driven mode for authentication during OOBE

C. Enable MDM auto-enrollment via GPO for automatic Intune enrollment post-join

D. Use PowerShell to set the join type explicitly with dsregcmd /join after provisioning

E. Configure Microsoft Entra device settings to allow users to join devices and set maximum devices per user to 0 for kiosks

Answer: A,C

Explanation: Selecting Microsoft Entra joined in the Autopilot profile Join to Microsoft Entra ID as setting ensures cloud-only join for self-deploying kiosks. Enabling MDM auto-enrollment via GPO for automatic Intune enrollment post-join applies if hybrid elements exist, but for pure Entra join, Intune auto-enrollment triggers automatically with P1/P2 licensing.

Question: 1230

Kiosk deployment: Autopilot Entra joined devices must install specific app before ESP completes. ESP set to block until selected apps installed. Assign via?

A. Devices > Enrollment Status Page > Blocking apps > Select kiosk app

B. Autopilot profile > Required apps list

C. Compliance policy > Actions for noncompliance > App install required

D. Dynamic group > App assignment > Required

Answer: A

Explanation: In ESP profile, "Block device use until these required apps are installed: Selected" > Select apps adds the kiosk app to blocking list, preventing desktop access until installation during Entra join ESP for self-deploy scenarios.

Question: 1231

Complex ASR scenario: Configure policy blocking credential stealing from LSASS (GUID: 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2), Office communication apps (26190899-1602-49e8-8b27-eb1d0a1ce869), script execution (d3e037e1-3eb8-44c8-a917-57927947596d) at Block level with path exclusions C:\Windows\Temp*.tmp, audit fallback after 7 days. Which GUIDs and settings are accurate?

A. ASR rule 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 Block, Exclude C:\Windows\Temp*.tmp

B. Rule 26190899-1602-49e8-8b27-eb1d0a1ce869 Warn, Script rule d3e037e1-3eb8-44c8-a917-57927947596d Audit

C. Integrate with antivirus Cloud extension

D. Set Throttle scanning CPU priority 4, End user notifications Enabled

E. Priority 0, Conflict resolution Highest

Answer: A,D

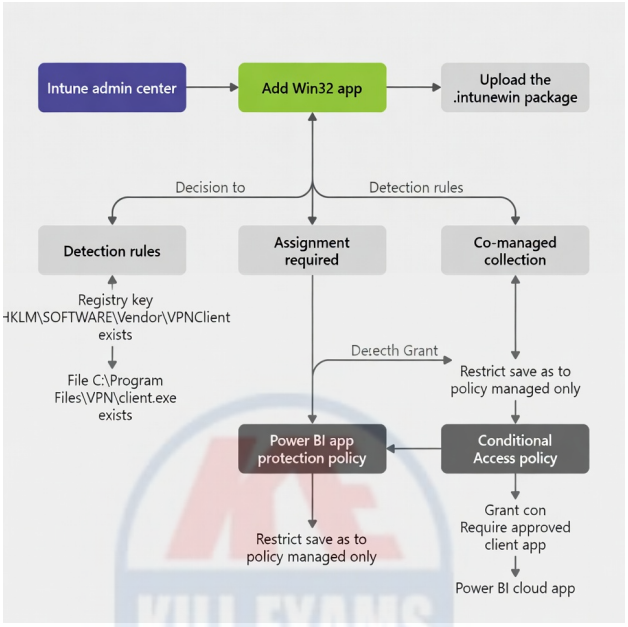
Explanation: ASR rule GUID 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 set to Block prevents LSASS credential dumping, a primary technique in lateral movement, with exclusions for temp files avoiding breaks. Throttling CPU priority to 4 and enabling end-user notifications balance security with usability during high-activity scans.

Question: 1232

Case study

Tailwind Traders has a mixed environment with Windows 11 co-managed devices and iOS/iPadOS user-enrolled BYO**D.** They deploy a custom

Win32 app for VPN client requiring detection rules based on registry key and file existence. They also deploy Microsoft Store for Business apps like Power BI and configure app protection for Power BI mobile to prevent save to unmanaged locations. Conditional Access requires approved client apps for Power BI service.



To update the Win32 VPN app automatically when new version is uploaded, what feature is used?

A. Automatic update in Win32 app settings

B. Microsoft Store auto-update

C. Device configuration for updates

D. App supersedence in Intune

Answer: D

Explanation: Use app supersedence in Intune to define the new VPN app version as superseding the older one, specifying uninstall behavior if needed, so Intune automatically deploys the updated version to devices with the previous app installed.

Question: 1233

You are deploying Cloud PKI to issue SCEP certificates to iOS devices for Wi-Fi authentication. You need to configure the Issuing CA to automatically revoke certificates when a device is wiped or retired from Intune. Which configuration element is essential for this automation to function?

A. Verifying that the SCEP profile has the "Certificate Revocation" setting enabled and points to the Cloud PKI CRL Distribution Point (CDP).

B. Enable the "Intune Certificate Connector" on a local Windows Server with the "Revocation Proxy" role active.

C. Set the "Revoke on Deletion" flag to "True" within the Cloud PKI Issuing CA properties in the Intune admin center.

D. Use a "Custom Configuration Profile" with an XML payload that targets the "com.apple.mobiledevice.passwordpolicy" payload with revocation triggers.

Answer: C

Explanation: Microsoft Cloud PKI provides native integration with the Intune device lifecycle. Within the properties of the Cloud PKI Issuing CA, there is a specific toggle for "Revoke certificates when device is deleted". When this is enabled, Intune automatically triggers a revocation request to the Cloud PKI service whenever a device is "Wiped", "Retired", or deleted from the Intune console. This ensures that the Certificate Revocation List (CRL) is updated immediately, preventing the decommissioned device from using its certificate to access corporate resources like Wi-Fi or VPN.

Question: 1234

For Android Enterprise fully managed, deploy private .apk as LOB with no Play visibility. Enable more volume controls in Managed Home Screen post-install. What supports this?

A. Add as Android LOB, assign required; use OEMConfig app for Managed Home Screen volume enhancements

B. Script to adjust

C. Device restrictions for volume

D. Managed Google Play approve private app

Answer: A

Explanation: Android LOB for private .apk ensures sideload control. New 2025 OEMConfig support for Managed Home Screen allows additional volume options in dedicated/fully managed profiles via configuration app.

Question: 1235

Intune ESP blocks apps until "device compliant." New Entra joined device pending. Accelerate?

A. Run Sync from Intune > Devices > Check status

B. Autopilot ESP: Apps=After

C. CA require compliant + hybrid

D. ESP profile: Block non-compliant, timeout 60min

Answer: A

Explanation: Manual sync post-join pushes compliance policy for ESP progress; hybrid unnecessary for pure Entra.

Question: 1236

A company has implemented Android Enterprise (AOSP) devices for a warehouse. You need to manage firmware updates using a specific manufacturer's FOTA provider. What are the two primary requirements to link Intune with a third-party FOTA provider like Zebra or Samsung?

A. A Google Play Store Developer account

B. A specialized connector or app from the manufacturer installed in Intune

C. A VPN tunnel between Intune and the FOTA server

D. Public IP addresses for all mobile devices

E. Device enrollment using "Corporate-owned dedicated device" mode

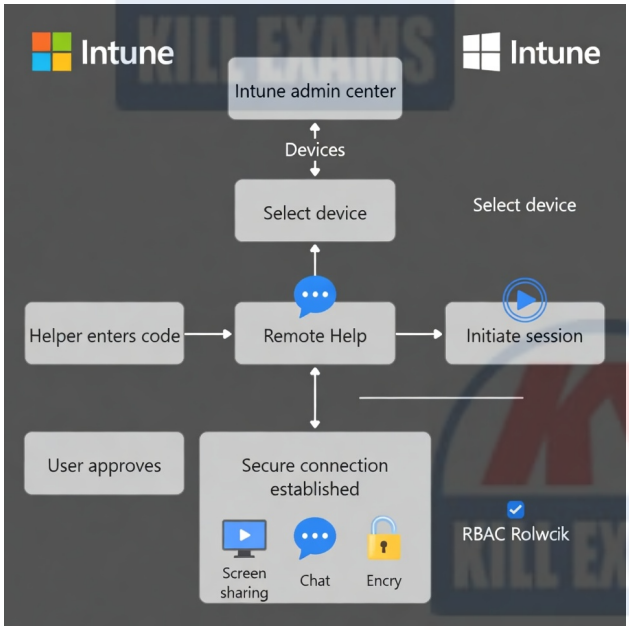
Answer: B,E

Explanation: Most advanced FOTA management requires the "Corporate-owned dedicated device" (formerly COSU) enrollment because it gives the administrator full control over system-level changes. Additionally, manufacturers like Zebra or Samsung require a specific service connector or a management app (like the Zebra LifeGuard over-the-air tool) to be integrated with Intune to bridge the communication between Intune's policies and the manufacturer's update servers.

Question: 1237

Case study

The helpdesk uses Intune Remote Help (Intune Suite) for secure troubleshooting on enrolled Windows devices. They require just-in-time access with role-based controls and session recording.



To enhance security during Remote Help usage, which features should be implemented?

A. Enable session recording for audit

B. Use just-in-time access via PIM

C. Require multi-factor authentication for initiation

D. Set time limits on sessions

E. Allow unattended access for kiosks

Answer: A,B,D

Explanation: Session recording provides audit trails for compliance. Time limits prevent prolonged access. Just-in-time access via Privileged Identity Management (PIM) adds approval workflows for elevated helpdesk actions.

Question: 1238

Which of the following is a key difference between Microsoft Entra join and Microsoft Entra registration?

A. Only Entra join supports Windows Hello for Business.

B. Only Entra registration requires a Global Administrator to perform.

C. Only Entra registration is supported on Windows 11 Home.

D. Only Entra join allows for SSO to cloud resources.

Answer: C

Explanation: Windows 11 Home edition lacks the enterprise features required to join a domain (either local or Entra ID). It does, however, support Microsoft Entra registration, which allows the device to be "known" to the directory for access to apps like Teams or Outlook without full management. Both types support SSO and Windows Hello for Business, though the implementation details differ.

Question: 1239

Windows 11 upgrade scenario requires blocking upgrade on devices with incompatible VPN software, defer quality 7 days post-upgrade. Which? (Select two.)

A. Enable safeguard for incompatible software

B. Use Autopilot reset for upgrade

C. Enable express updates

D. Use feature update policy targeting

E. Set quality update deferral in post-upgrade ring

Answer: A,E

Explanation: Enable safeguard for incompatible software prevents upgrade on devices with known blocking apps like legacy VPN. Set quality update deferral in post-upgrade ring defers patches after successful feature update.

Question: 1240

For compliance auditing, bulk sync 500 devices to force policy refresh after a new endpoint protection profile deployment. What is the maximum per bulk operation and best practice? (Select two)

A. Initiate sync post-retire to confirm management removal

B. Bulk sync supports up to 100 devices per action

C. Combine with bulk restart to ensure kernel-level policy application

D. Prefer individual sync for accuracy in large sets

E. Use multiple bulk sync batches and monitor in Device actions

Answer: B,E

Explanation: Bulk device actions limit is 100 devices per operation for sync, requiring batching for larger sets like 500. Execute multiple batches and monitor status in the Device actions section for completion and errors.

Question: 1241

Tunnel MAM gateway logs "Auth failure 403" for Defender app on Android, despite SCEP client cert. Site identity cert SAN=tunnel.contoso.com, split DNS. Firewall ESP 50/UDP? Which profile dep?

A. Deploy SCEP before VPN profile dependency, open IP protocol 50/ESP, 51/AH

B. TCP/UDP 1701

C. Root cert only

D. App config VPN=Always

Answer: A

Explanation: VPN profile depends on SCEP (client auth cert) and root; IPsec requires ESP (50), AH (51) for gateway auth 403 resolution, complementing 443/500/4500. Split DNS aids MAM.

Question: 1242

Detection rule for Win32 app uses script checking registry multi-string value contains "Installed". What script exit ensures detection?

A. File hash only

B. PowerShell: if value contains "Installed", exit 0 else 1

C. Exit 3010 on success

D. MSI code

Answer: B

Explanation: Custom script detection requires exit 0 for present/successful install; PowerShell Get-ItemProperty checking multi-string for keyword confirms installation accurately.

Question: 1243

Your company implements Windows Hello for Business in a "Cloud Kerberos Trust" deployment. You need to ensure that the "Use cloud trust for on-premises authentication" setting is enabled. Where is this configured in Intune?

A. Microsoft Defender for Identity settings

B. Device Restrictions profile

C. Identity Protection configuration profile

D. Windows Hello for Business enrollment profile

Answer: D

Explanation: The "Use cloud trust for on-premises authentication" setting is part of the Windows Hello for Business (WHfB) node within the Intune enrollment settings or the Identity Protection profile, facilitating passwordless access to on-premises resources.

Question: 1244

In Intune, automatic enrollment for Windows fails for some users despite correct scope. Devices show as Microsoft Entra joined but not MDM enrolled. What must be checked? (Choose two.)

A. Set MAM scope to All

B. Check if devices are blocked by enrollment restrictions

C. Verify MDM discovery URL is set to https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

D. Ensure users have Microsoft Entra ID P1/P2 for automatic join features

E. Force Intune sync from Company Portal

Answer: B,C

Explanation: The correct MDM discovery URL must be configured in Microsoft Entra ID for automatic enrollment to function. Enrollment restrictions may block specific devices or platforms even if scope allows.

Question: 1245

Your security architecture team deploys Microsoft Cloud PKI within Intune Suite as a two-tier hierarchy (Root CA imported, Issuing CA cloud-hosted). They configure SCEP certificate profiles for device authentication on Wi-Fi and user certificates for VPN. Which three use cases are optimally addressed by this implementation?

A. Full revocation propagation and CRL/OCSP support for certificates issued to both managed and unmanaged endpoints

B. Automatic issuance and renewal of device certificates via SCEP for 802.1x Wi-Fi authentication on managed Windows, iOS, and Android devices

C. Manual certificate issuance to non-managed or third-party devices outside Intune enrollment

D. Integration with Windows Hello for Business and Microsoft 365 apps requiring certificate-based authentication for seamless sign-in

E. Secure certificate-based VPN authentication using user certificates to eliminate password-based exposure in remote access scenarios

Answer: B,D,E

Explanation: Cloud PKI issues SCEP-based device certificates automatically for managed platforms, enabling secure 802.1x Wi-Fi with lifecycle management. User certificates support VPN authentication securely without passwords. It integrates natively with WHfB and M365 apps for certificate-backed sign-in on Intune-managed devices.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions Based on Current Exam Objectives

Killexams.com provides exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Exam MCQs (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.