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

KILL EXAMS

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

PASS

killexams.com

Microsoft

MS-102

Microsoft 365 Administrator

ORDER FULL VERSION

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

Question: 1276

Your organization implements a "Zero Trust" model. You need to create a Conditional Access policy for all users. The policy must satisfy the following: 1. Block access from specific high-risk countries. 2. Require MFA for all other locations. Which three configurations are required in the Conditional Access policy?

A. A 'Block' grant control assigned to the specific countries location
B. An 'All Users' assignment
C. A 'Require multifactor authentication' grant control for 'Any location'
D. Exclude the 'Trusted Locations' from the MFA requirement
E. A Named Location containing a list of IP ranges for blocked countries

Answer: A,B,E
Explanation: Defining Named Locations allows the system to identify the geographic origin of the IP address. By assigning 'All Users' to a policy that uses these locations in the 'Conditions' section, you can then apply a 'Block' grant control to prevent any access from those specific regions.

Question: 1277

You need to interpret Activity log for a policy match on bulk share. What severity influences notification?

A. App risk score
B. IP reputation
C. User role
D. Policy severity level configured determines email alert propagation

Answer: D
Explanation: Alerts section in policies uses the assigned policy severity (Low/Medium/High) to determine if matches trigger notifications or emails to admins.

Question: 1278

Your hybrid tenant uses pass-through authentication. Users report intermittent SSPR failures with error "Authentication method not supported." The Authentication methods policy enables Microsoft Authenticator and Email OTP for all users. What hybrid-specific configuration is required to resolve this?

A. Install the on-premises Password Protection DC Agent on all domain controllers
B. Enable password writeback in Microsoft Entra Connect to allow cloud-initiated resets to sync back
C. Configure the legacy SSPR policy to include the same methods until migration completes
D. Set the number matching feature in Authenticator to mandatory for hybrid users

Answer: B
Explanation: In hybrid environments without password writeback enabled in Microsoft Entra Connect, SSPR changes made in the cloud cannot propagate to on-premises Active Directory when using pass-through authentication or PTA, leading to unsupported method errors or failed resets.

Question: 1279

You are the Microsoft 365 administrator for a company with 15,000 users. Microsoft Entra ID Protection detects leaked credentials for several high-privilege accounts. You need to enforce mandatory password changes only for affected users without impacting others, using risk-based policies. Which policy configuration achieves this with the least administrative overhead?

A. Configure a sign-in risk policy set to Medium and High risk levels requiring password change
B. Implement a custom Conditional Access policy blocking sign-in for leaked credentials
C. Enable a user risk policy with High risk level set to "Change password immediately"
D. Configure Microsoft Entra Password Protection to ban leaked password hashes organization-wide

Answer: C
Explanation: The user risk policy in Microsoft Entra ID Protection, when set to High risk level and configured to "Change password immediately," forces affected users (those with leaked credentials) to reset their password upon next sign-in, leveraging risk detection without broad impact.

Question: 1280

Implementing MFA via Conditional Access for sales team (group sales-execs) accessing Dynamics 365 Finance app from BYO**D.** Requirements: Microsoft Authenticator push + number matching, FIDO2 keys allowed, exclude if device marked compliant via Intune. Policy conditions: Client apps Modern auth only. Which three implementations?

A. Conditions > Device platforms All > Filter "complianceState ne 'compliant'"; Client apps > Modern authentication
B. Authentication context > Require number matching Yes; Allowed methods > Authenticator push, FIDO2
C. Assign Intune policy: Device compliance > Mark compliant for corporate cert presence
D. Enable > Report-only 14 days; Monitor sign-ins | where AppDisplayName == "Dynamics 365" and Status.ErrorCode == 53003

E. Target > Groups sales-execs; Apps > Dynamics 365 Finance; Grant > Require MFA with Authenticator push, number matching

Answer: A,B,E
Explanation: Targeting sales group and Dynamics app with MFA requiring Authenticator push and number matching secures high-value access appropriately. Conditions excluding compliant devices via filter and modern auth only prevent legacy client issues. Enabling authentication context with FIDO2 support provides phishing-resistant MFA options.

Question: 1281

Your company discovers high-volume traffic to previously unknown apps via firewall logs. You enable Cloud App Discovery in Microsoft Defender for Cloud Apps and upload the logs for analysis. After processing, the dashboard shows several high-risk apps with risk scores below 5. What is the next step to automatically generate alerts for any new app discovered with a risk score lower than 4 and more than 100 users accessing it?

A. Enable automatic sanctioning for apps with risk score >5
B. Configure a session policy with Block access for apps with risk score <4
C. Create an anomaly detection policy with Risky app usage template
D. Create an app discovery policy using the New risky app template and set threshold to risk score <4 and users >100

Answer: D
Explanation: App discovery policies use templates like New risky app to monitor Cloud Discovery logs and trigger alerts when new apps meet criteria such as risk score below a threshold (e.g., <4) and user count exceeding a value (e.g., >100), automating detection of emerging Shadow IT threats without manual review.

Question: 1282

In your tenant, Microsoft Entra ID Protection has detected several medium sign-in risk events involving token replay attacks from unfamiliar features. You need to implement a Conditional Access policy that requires phishing-resistant MFA (such as FIDO2 or certificate-based) only when sign-in risk is medium or high, while allowing standard MFA for low-risk sign-ins from known devices.What setting combination achieves this with minimal administrative overhead?

A. Enable the built-in risk-based policy in ID Protection and set sign-in risk to Require phishing-resistant MFA for Medium/High
B. Configure user risk policy to block Medium/High and rely on ID Protection automated remediation
C. Create a sign-in risk-based Conditional Access policy with Medium and High risk levels requiring

phishing-resistant MFA grant control

D. Use a standard Conditional Access policy with sign-in risk condition set to Medium/High and Grant: Require authentication strength - Phishing-resistant MFA

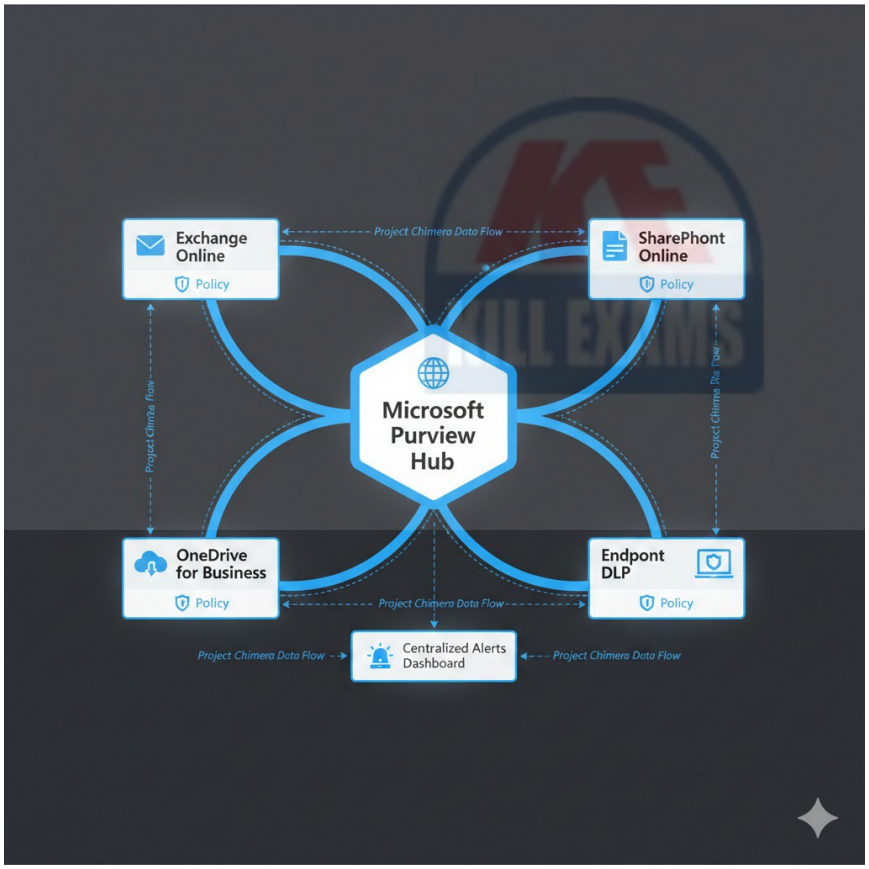
Answer: D

Explanation: The Conditional Access sign-in risk condition (requiring Entra ID P2) allows integration with real-time risk signals from ID Protection. By setting the condition to include Medium and High sign-in risk levels and using the Grant control for "Require authentication strength" with a custom strength policy defined as phishing-resistant methods only, the policy enforces stronger MFA precisely when risk is elevated, without affecting low-risk sign-ins.

Question: 1283

Case study

Fabrikam, Inc. is a global manufacturing company transitioning to a highly regulated data environment. The organization uses Microsoft 365 E5. The IT department needs to secure intellectual property related to "Project Chimera," which involves CAD designs and chemical formulas. The legal department requires that all emails containing these formulas be retained for seven years, while drafts stored in OneDrive should be deleted after three years of inactivity. You are the Microsoft 365 Administrator tasked with implementing these controls using Microsoft Purview.



You need to monitor the effectiveness of the new "Project Chimera" sensitivity labels. You want to see

which specific files in a SharePoint site have the label applied and who applied them. Which tool should you use?

A. Label Analytics dashboard
B. Microsoft Defender for Cloud Apps
C. Activity explorer
D. Content explorer

Answer: D
Explanation: Content explorer is the specific tool in Microsoft Purview that allows administrators to drill down into specific locations, such as SharePoint sites, to view the actual files that have been classified and labeled, providing visibility into the specific content.

Question: 1284

A legal firm requires a data lifecycle management strategy for SharePoint Online. You must ensure that documents in the "Litigation" site collection are kept for seven years after they are last modified. After the seven years, a group of legal users must manually approve the deletion. Which three components must be configured to meet these requirements?

A. A retention label policy of type "Adaptive"
B. A retention policy applied to the SharePoint site
C. A retention label policy of type "Static"
D. Retention settings set to "Start the retention period based on: when items were last modified"
E. A retention label configured with a disposition review

Answer: C,D,E
Explanation: A retention label is necessary when a disposition review is required for manual approval of deletion. By setting the retention period to trigger based on the last modified date, the seven-year clock resets every time a document is edited. A static retention label policy is the standard method for publishing these labels to specific SharePoint site collections to ensure they are available for application to documents.

Question: 1285

A security audit reveals that many malicious emails are bypassing filters because they are sent from trusted cloud service IP addresses. You want to implement 'Standard' preset security policies to ensure Microsoft's best practices are applied. Which two statements are true regarding 'Standard' and 'Strict' preset security policies?

A. Preset policies are always applied before custom policies

B. You must assign users to the preset policy for it to take effect
C. 'Strict' policies have more aggressive 'Bulk Email Threshold' (BET) settings than 'Standard'
D. Preset policies take precedence over the Default policies
E. You can modify individual settings within a preset policy

Answer: C,D
Explanation: Preset security policies (Standard and Strict) are designed to apply Microsoft's recommended settings quickly. They take precedence over Default policies. The "Strict" profile is more aggressive, specifically setting the Bulk Email Threshold (BET) to a lower value (typically 4 or 5) compared to the "Standard" profile (typically 6), making it harder for bulk mail to reach the inbox.

Question: 1286

You are managing a Microsoft 365 tenant with several thousand users. The executive team wants to ensure that users cannot see the "Add-ins" button in the Office ribbon and that users are prevented from purchasing their own third-party subscriptions using their corporate identity. Which settings in the Microsoft 365 admin center must be modified?

A. Run the Set-MSOrgServiceSettings cmdlet with the -UserPurchasableServiceList parameter.
B. Disable "Allow users to access the Office Store" under Settings > Org settings > Services > User owned apps and services.
C. Set the "Self-service purchases" flag to "Disabled" for all relevant products via the MSCommerce PowerShell module.
D. Disable "Let users install Apps for Office" under Settings > Org settings > Services > Apps.
E. Execute the Update-MgPolicyAuthorizationPolicy PowerShell cmdlet with the -AllowedToCreateApps parameter set to $false.

Answer: B,C
Explanation: The "User owned apps and services" setting in the Org settings menu directly controls whether users can access the Office Store to browse and install add-ins. To prevent the purchase of individual subscriptions (self-service purchases) like Power BI or Visio, an administrator must use the MSCommerce PowerShell module to disable the policy for specific product IDs.

Question: 1287

You have configured multiple channel profiles in cloud update with different exclusion windows for pilot versus production. A production profile unexpectedly receives an update during an exclusion window. What is the most likely cause?

A. Global cloud update setting override
B. Device group membership conflict

C. Pilot profile assignment overlap
D. Exclusion window misconfiguration on profile

Answer: D
Explanation: Exclusion windows are profile-specific; a misconfiguration or incorrect application of the window to the production channel profile would allow updates to proceed during the intended exclusion period, bypassing the intended protection.

Question: 1288

Contoso uses Microsoft Entra ID P2 and has high-risk sign-ins from legacy authentication protocols. You plan a Conditional Access policy to enforce phishing-resistant MFA only for administrators accessing Azure resources from high sign-in risk locations. Which authentication strength should you configure in the policy's Grant control?

A. Phishing-resistant MFA strength
B. Passwordless MFA strength
C. Multifactor authentication strength
D. Custom authentication strength with certificate-based

Answer: A
Explanation: Phishing-resistant MFA strength in Conditional Access requires methods like FIDO2 security keys, Windows Hello for Business, or certificate-based authentication that resist phishing attacks, ideal for administrators in high-risk scenarios. This built-in strength ensures only phishing-resistant methods satisfy the policy when combined with sign-in risk and location conditions.

Question: 1289

You need to convert a standard user mailbox into a shared mailbox to save on licensing costs while keeping the data. Which two conditions must be met?

A. The user account must remain in the directory (though it can be disabled)
B. The user must have a valid license at the time of conversion
C. The user account must not have an Archive mailbox enabled
D. The user's mailbox must be smaller than 100 GB
E. The user account must be deleted before conversion

Answer: A,B
Explanation: To convert a mailbox, the user account must still exist in the directory because the shared mailbox remains linked to that user object. The user must also be licensed at the moment of conversion; once the conversion to a shared mailbox is complete, the license can be removed, provided the mailbox is

under 50 GB (not 100 GB).

Question: 1290

A company wants to move to a purely passwordless environment. They have decided to use the Microsoft Authenticator app. Which three requirements must be met for a user to successfully use "Phone Sign-in"?

A. The device must be registered in Microsoft Entra ID
B. The user must have the "Passwordless" mode enabled in the Authenticator method policy
C. The user must have at least one password reset performed in the last 90 days
D. The Microsoft Authenticator app must be set as the default MFA method
E. The user must have a PIN or biometric lock enabled on their mobile device

Answer: A,B,E
Explanation: Phone sign-in (passwordless) requires the device to be registered (Workplace Join) to the tenant. The Authenticator policy must explicitly allow passwordless mode. Finally, for security, the mobile app requires a device-level lock (PIN/biometrics) to protect the private key used for the sign-in.

Question: 1291

Your tenant has insider risk signals enabled (preview). A Conditional Access policy must block access if insider risk is detected alongside medium user risk for finance users accessing sensitive SharePoint sites. Which condition combination achieves this with the least policy sprawl?

A. User risk = Medium only → Block
B. User risk = Medium and Insider risk detected → Block
C. Separate policies for user risk and agent risk
D. Sign-in risk = Medium and Insider risk → Require MFA

Answer: B
Explanation: Conditional Access supports insider risk (preview) as a condition alongside user risk from Entra ID Protection. Combining User risk = Medium and Insider risk detected in one policy with Block access control enforces zero trust for high-sensitivity scenarios without multiple policies, using integrated signals for contextual blocking.

Question: 1292

An administrator wants to create a Microsoft 365 group for project collaboration with dynamic membership for all users in "Marketing" department but exclude contractors identified by extensionAttribute1 = "Contractor". What is the correct membership rule syntax?

A. user.department equals "Marketing" OR user.extensionAttribute1 not equals "Contractor"
B. user.department -eq "Marketing" and not(user.extensionAttribute1 -eq "Contractor")
C. (user.department -eq "Marketing") and (user.extensionAttribute1 -not "Contractor")
D. (user.department -eq "Marketing") -and (user.extensionAttribute1 -ne "Contractor")

Answer: D
Explanation: Dynamic membership rules use -eq/-ne operators with parentheses for grouping and -and/-or for logic. The syntax (user.department -eq "Marketing") -and (user.extensionAttribute1 -ne "Contractor") correctly includes Marketing department members while excluding contractors.

Question: 1293

Case study
Wingtip Toys, a consumer goods firm with 1,500 users, detected insider threat via anomalous Teams shares. Defender XDR incidents included email rules, endpoint processes, and Cloud Apps alerts. Secure Score at 710, simulations pending review. Admin to manage simulations, policies, hunting.

What is the single correct restricted entities management?

A. Block users with repeated sim failures >3
B. No restrictions for insiders

C. Manual review only for High risk
D. Auto-unblock after 7 days

Answer: A
Explanation: Blocking users with >3 sim failures enforces training compliance.

Question: 1294

You need to perform a "Point-in-time" restore of a user's OneDrive account using Microsoft 365 Backup. The user deleted several files three weeks ago and recently realized they were needed. Which factors should you consider?

A. You cannot restore data that was deleted more than 14 days ago.
B. The restore operation will generate a "Restore Report" upon completion.
C. You can choose to restore the files to a new folder in the user's OneDrive instead of overwriting.
D. Restoration will restore the entire OneDrive to the state it was in at the selected timestamp.
E. The files must still be in the OneDrive "Recycle Bin" for the restore to work.

Answer: B,C,D
Explanation: Point-in-time restoration effectively "rewinds" the OneDrive to a specific moment. The system provides a report to verify what was processed. To prevent data loss of new files created since the backup point, you can opt to restore the data to a new folder.

Question: 1295

An administrator is trying to troubleshoot why certain cloud activities are not appearing in the Microsoft Defender for Cloud Apps activity log. Which three reasons could explain the missing data?

A. The user performing the activity is not assigned a Microsoft 365 E5 license
B. The specific activity type is not supported by the app's API
C. The activity occurred before the app connector was established
D. The user is using a Private/Incognito browser mode
E. The app connector for that specific service is not connected

Answer: B,C,E
Explanation: Data ingestion depends on an active app connector; if it's disconnected or was established after the event, the data won't be there. Additionally, the amount of data captured is limited by what the specific SaaS provider's API exposes; not every action in a third-party app is logged by their API.

Question: 1296

In troubleshooting authentication issues, a user's sign-in fails with code 50058 after SSPR success. What indicates the root cause?

A. Conditional Access requires re-registration post-reset
B. The new password violates Password Protection but was allowed in Audit
C. Password writeback failed in hybrid, causing cloud/on-prem mismatch
D. SSPR registration invalidated existing MFA sessions

Answer: C
Explanation: In hybrid with PTA or no writeback, successful cloud SSPR does not update on-premises password, leading to subsequent authentication failures (code 50058 often mismatch-related) as the credentials diverge.

Question: 1297

Case study
Northwind Traders, a logistics company with 4,000 mobile workers, suffered a BEC attack evading filters, leading to wire fraud alerts in Defender XDR. Cloud App Discovery revealed shadow IT (Dropbox), endpoint configs lacked ASR, and simulations showed 60% phish success. Admin to configure alerts, endpoints, and discovery.

What single alert policy setting for BEC?

A. No notifications for finance group
B. High severity for 'Unusual volume of transfers' category
C. Weekly aggregation only
D. Low severity to reduce noise

Answer: B
Explanation: High severity for 'Unusual volume of transfers' ensures BEC alerts prioritize SOC triage.

Question: 1298

Your company uses Activity explorer to monitor how sensitivity labels are being applied to files in OneDrive for Business. You notice a high volume of "Label removed" events for the "Secret" label. You need to identify which users are performing these actions and whether they are providing justifications. Which three filters should you apply in Activity explorer to isolate this data?

A. Label: Secret
B. Activity: Label removed
C. File extension: .docx and .pdf
D. User: Specific administrative accounts
E. Activity: Label upgraded

Answer: A,B,D
Explanation: Filtering by the specific "Label removed" activity allows you to see exactly when protection is being stripped from files. Combining this with a filter for the "Secret" label focuses the results on your highest-risk data. Filtering by specific users or reviewing the user column in the filtered results identifies the individuals responsible, and the Activity explorer detail pane will display the justification text provided by those users during the downgrade.

Question: 1299

You are reviewing the Microsoft Defender XDR "Threat Analytics" report for a newly discovered 0-day vulnerability. The report indicates that several devices in your organization are "Incomplete" for remediation. You need to use the "Exposure Management" tools to assess the business risk. Which two actions are required to find the specific configuration weaknesses?

A. Open the "Vulnerability Management" dashboard and filter by the specific CVE ID associated with the 0-day
B. Run a "Guided Hunting" query provided in the Threat Analytics "Analyst Report" to find vulnerable process versions

C. Set the "Risk Level" of all vulnerable devices to "High" in the device inventory manually
D. Use the "Exposure Graph" to see if the vulnerable devices have "Permissions to manage" sensitive cloud resources
E. Use the "Cloud App Discovery" to see if the 0-day is being exploited in third-party SaaS apps

Answer: B,D
Explanation: The "Analyst Report" within Threat Analytics frequently provides pre-written KQL queries specifically designed to detect the presence or exploitation of a new vulnerability. Using the Exposure Graph to check for permissions on sensitive cloud resources allows the admin to quantify the risk; a vulnerable device with high-level access to the cloud environment represents a significantly higher risk to the organization than an isolated workstation.

Question: 1300

Your organization requires alerting on any new cloud app discovered via Cloud Discovery with daily traffic over 2 GB and risk score under 6. The app must be reviewed before sanctioning. Which app discovery policy template and severity setting achieves this?

A. New high volume app template with Medium severity alert
B. Cloud storage app compliance check with Critical severity
C. New popular app template with Low severity
D. New risky app template with High severity and user threshold none

Answer: D
Explanation: The New risky app template in app discovery policies triggers alerts for newly discovered apps with low risk scores (under 6) and high usage (configurable traffic or user thresholds like >2 GB daily), set to High severity to ensure immediate review before any sanctioning decision.

Question: 1301

Troubleshooting Microsoft Entra Cloud Sync: Agent shows "unhealthy" in portal. Logs indicate proxy authentication failure. What to check?

A. Proxy server credentials and configuration in agent settings
B. License
C. Firewall rules only
D. AD permissions

Answer: A
Explanation: If a proxy is used, the provisioning agent requires correct proxy address, port, and authentication credentials configured during install or via config file for health and connectivity.

Question: 1302

In reports section of Defender XDR, issues show unaddressed misconfigurations affecting Secure Score. What is the response workflow?

A. Export without action
B. Suppress report issues
C. Review issues, select linked Secure Score action, implement, and monitor score increase
D. Accept all risks

Answer: C
Explanation: Defender XDR reports identify issues like misconfigurations. Responding involves reviewing, implementing linked Secure Score improvement actions, and monitoring verification for score improvement.

Question: 1303

You need to create a shared mailbox named "Info" and ensure that three specific users (User1, User2, and User3) can read the emails. You also want to ensure that any reply sent from this mailbox shows the sender as "Info". Which two cmdlets or actions are required?

A. New-MgUser -DisplayName "Info" -MailEnabled $true
B. Set-Mailbox -Identity "Info" -GrantSendOnBehalfTo User1, User2, User3
C. Add-RecipientPermission -AccessRights SendAs
D. New-Mailbox -Shared -Name "Info"
E. Add-MailboxPermission -AccessRights FullAccess

Answer: C,E
Explanation: After creating the mailbox, the Add-MailboxPermission cmdlet with the "FullAccess" right is required for the users to open and read the emails. To ensure the sender appears as "Info" (and not "User1 on behalf of Info"), the Add-RecipientPermission cmdlet with the "SendAs" right must be used.

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.