

Boost up Your Certification Score

Forcepoint

DSPM- Deploy-and-Administer

Certified Forcepoint DSPM - Professional: Deploy and Administer Exam



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Visit us at: <https://www.examsboost.com/test/dspm-deploy-and-administer>

Latest Version: 6.0

Question: 1

DRAGDROP:

Place the following steps in the correct order to add a user to Forcepoint DSPM.

Steps to be ordered:

- 1. Select Administrators.
- 2. Set realm to gv.
- 3. Navigate to Administration > User Management.
- 4. Select Join Groups.
- 5. Fill in the necessary user information.
- 6. Select Users then Add user.

Correct order (as shown in the preview):

3. Navigate to Administration > User Management.
2. Set realm to gv.
6. Select Users then Add user.
5. Fill in the necessary user information.
4. Select Join Groups.
1. Select Administrators.

Answer:

Explanation:

Correct order: 3 → 2 → 6 → 5 → 4 → 1

Navigate to Administration > User Management .

Set realm to gv .

Select Users , then Add user .

Fill in the necessary user information.

Select Join Groups .

Select Administrators .

Forcepoint DSPM user administration for a standalone deployment is performed through the Keycloak-based user management workflow. The sequence begins by entering the DSPM administration area and opening User Management , which places the administrator in the identity-management context used to control DSPM UI access. The next critical step is selecting the gv realm. Forcepoint documentation specifically instructs administrators to select the gv realm after logging into Keycloak and warns against changing settings in the Master realm, because the DSPM application authorization model is tied to the gv realm rather than the default administrative realm.

After the correct realm is active, the administrator creates the account by selecting Users , choosing Add user , and entering required identity fields such as username, email, first name, and last name. Once the user object exists, access is completed through RBAC group membership. Forcepoint's RBAC guidance

recommends group-based role assignment: navigate to the user, open the Groups area, search/select the appropriate group, and click Join . Selecting Administrators grants the required administrative group membership and resulting DSPM access.

Question: 2

Which of the following are actions that can be performed from the Enterprise Search page? Select three.

- A. Revoking user permissions.
- B. Exporting reports.
- C. Moving risky files to a private folder.
- D. Manually changing the assigned risk.
- E. Manually verifying ML classification.

Answer: A, B, E

Explanation:

The correct selections are Revoking user permissions , Exporting reports , and Manually verifying ML classification . The Enterprise Search page is the primary file-level investigation view in Forcepoint DSPM. It lists scanned and cataloged files, allows filtering through standard filters or GQL, and provides operational actions against the returned results. Forcepoint states that Enterprise Search allows users to filter file data, save frequently used filters, customize columns, and generate meaningful reports. It also provides an EXPORT button that creates a CSV or JSON download of the filtered data.

Revoking permissions is also supported as a data-governance action. Forcepoint documents that administrators can view or modify file permissions and access rights from the file Actions menu, and supporting documentation identifies required permissions for revoke operations in Microsoft repositories.

Manual classification validation is explicitly available from the Enterprise Search hamburger menu.

Forcepoint states that to adjust a file's machine-learning classification, the user selects Manually verify classification , modifies the ML-suggested classification, and saves the change.

The incorrect choices are outside this specific Enterprise Search action set. Moving risky files to a private folder is not the standard named Enterprise Search action in this workflow, and assigned risk is not manually changed from the page. References/topics: Enterprise Search, Exporting Data, Permissions & Access Rights, Manual ML Classification Verification .

Question: 3

DRAGDROP:

Provide the matching definitions for these Forcepoint DSPM Controls Orchestration terms:

Workflow Configuration Tool	Establish criteria to identify data policy violations, data handling irregularities, and other anomalies.
Rule-Based Automation	Review events and manage rules through cards.
Notification System	Triggered rules can be configured to generate alerts and send them to webhooks to ensure prompt action.
Incident Management	Allows the creation of GQL syntax rules with conditions for organizational files and users.

Answer:



Explanation:

Workflow Configuration Tool → Allows the creation of GQL syntax rules with conditions for organizational files and users.

Rule-Based Automation → Establish criteria to identify data policy violations, data handling irregularities, and other anomalies.

Notification System → Triggered rules can be configured to generate alerts and send them to webhooks to ensure prompt action.

Incident Management → Review events and manage rules through cards.

Controls Orchestration in Forcepoint DSPM is the policy automation layer used to convert data-risk criteria into reviewable operational events. The Workflow Configuration Tool is represented by the rule-building interface under Policy Center > Controls Orchestration, where administrators define datasets, ownership, rule conditions, and GQL logic for organizational files, trustees, or agent activities.

Forcepoint states that rules are created to identify data matching specific criteria and are applied during scans of the selected dataset.

Rule-Based Automation describes the criteria-driven detection model. Administrators establish rules that identify policy violations, data-handling irregularities, or other anomalies that require attention.

Notification System maps to the ability to configure triggered rules to send external notifications, including webhook-based alerts, when matching data is detected. Incident Management maps to the Incidents workflow: Forcepoint states that each rule is automatically added as a card in the Incidents tab, and selecting the card takes the user back to the associated rule. References/topics: Policy Center, Controls Orchestration, GQL Conditions, Notifications, Webhooks, Incidents.

Question: 4

DRAGDROP:

Match each export option with an appropriate use case:



Answer:

Export a Dashboard in PDF format	Export a Dashboard in PDF format
Export a Dashboard in JSON format	Export Enterprise Search results in CSV format
Export Enterprise Search results in CSV format	Export Enterprise Search results in JSONL format
Export Enterprise Search results in JSONL format	Export a Dashboard in JSON format

Explanation:

Export a Dashboard in PDF format → For analysis by other users

Export a Dashboard in JSON format → To duplicate a dashboard in another Forcepoint DSPM deployment

Export Enterprise Search results in CSV format → To import data into a spreadsheet or database

Export Enterprise Search results in JSONL format → To import data into a SIEM solution

Forcepoint DSPM uses different export formats for different operational purposes. A Dashboard PDF export is intended for human-readable sharing, review, and offline analysis. PDF is best when the dashboard needs to be distributed to managers, auditors, analysts, or department stakeholders who need a static visual report rather than a reusable configuration object. Forcepoint documents dashboard export capability as supporting PDF and JSON export from the dashboard interface.

A Dashboard JSON export preserves the dashboard definition rather than just the visual output. This makes JSON the correct format when the goal is to duplicate or migrate a dashboard into another Forcepoint DSPM deployment, because the dashboard structure, layout, panels, widgets, and configuration can be reused.

For Enterprise Search, CSV is the correct format for spreadsheet or database workflows. CSV is tabular, broadly compatible, and suited for Excel-style analysis, reporting, joins, and external data review.

Forcepoint documents Enterprise Search export as producing CSV or JSON downloads of filtered data.

JSONL is most appropriate for SIEM ingestion because each line can represent an individual structured event or record, making it easier for log pipelines and event-processing systems to parse at scale.

References/topics: Analytics Export, Dashboard Export, Enterprise Search Export, CSV, JSON/JSONL, SIEM Integration .

Question: 5

What is the role of the File Audit Log in Forcepoint DSPM?

- A. To display who has access to the file.
- B. To display the number of discovered files from a data scan.
- C. To display who has last accessed the file.
- D. To display the status of data scanning and any errors.

Answer: D

Explanation:

The correct answer is D. To display the status of data scanning and any errors . In Forcepoint DSPM, the File Audit Log is tied to scan processing and file-level scan events. Forcepoint's GQL reference defines the File Audit Log as "events associated with scanning of files," and lists fields such as source , eventType , functionalityName , moduleName , createdAt , message , path , fileId , scanId , and configurationId .

Those fields are designed to explain what happened to a file during the scan/classification process, including the relevant scan, module, event, and message detail.

This aligns with the scan analytics workflow. Forcepoint documents that when files are not classified, the interface can show the event indicating the classification failure, the file path, and the reason for the failure. It then allows the user to view the file audit log filtered by not-classified events, scan, and reason.

The other options describe different DSPM views. File access permissions are handled through access governance, discovered-file totals appear in scan analytics summaries, and last access information is a separate file activity or metadata concept. References/topics: Scan Analytics, File Audit Log, GQL File Audit Log Dataset, Scan Events, Classification Errors .

Question: 6

Which of the following describes a use case for Forcepoint DSPM pattern matching?

- A. Identifying personally identifiable information in Outlook and Gmail emails.
- B. Identifying and redacting personally identifiable information on OneDrive.
- C. Identifying personally identifiable information on SharePoint.
- D. Identifying and encrypting personally identifiable information on Google Drive.

Answer: C

Explanation:

Forcepoint DSPM pattern matching is used to identify defined pieces of information inside scanned content by applying regular expressions. The documented function is discovery and classification: pattern matching identifies particular information in a document by using RegEx that attempts to match file content. This makes identifying personally identifiable information on SharePoint the correct use case. SharePoint is a supported Microsoft data source for scanning, and Forcepoint specifically documents SharePoint Online as a connector used to scan SharePoint accounts and apply classification tags to files containing sensitive data stored in SharePoint.

The key distinction is that pattern matching does not perform remediation actions such as redaction or encryption. Options B and D therefore overstate the capability: Forcepoint DSPM may discover and classify sensitive data that later informs controls, but the pattern itself is not a redaction or encryption engine. Option A is less precise in this context because the question is testing the canonical pattern-matching use case against scanned documents and repositories, while the strongest documented repository example among the choices is SharePoint. Pattern configuration can also assign classification, compliance, and distribution tags when a RegEx is detected, such as GDPR/PII tagging for identifiers. References/topics: Pattern Matching, RegEx, Compliance Tags, SharePoint Scanning, Sensitive Data Classification .

Question: 7

When creating a Detector, which field allows you to exclude specific criteria from the search?

- A. Not contain
- B. Not Add

- C. Except
- D. Exclude

Answer: A

Explanation:

The correct answer is A. Not contain . In Forcepoint DSPM, detector creation uses inclusion and exclusion logic to control what should trigger a detector match. The Contain field defines the positive match criteria: the keywords, phrases, regular expressions, extensions, or path terms that the detector should search for. The Not Contain field provides the negative condition: terms or criteria that should be ignored even when the broader detector logic would otherwise match.

Forcepoint's DSPM documentation for Content Detectors states that if there are terms the detector should ignore, they are set in the Not Contain field. The same concept appears in Path Detectors , where administrators define the search method, populate Contain with triggering terms, and then use Not Contain to exclude terms from matching.

This matters operationally because detectors can otherwise generate excessive or misleading matches. For example, a detector looking for payroll-related content may include "salary" or "compensation" in Contain , while excluding harmless template, archive, or test terms in Not Contain . Not Add , Except , and Exclude are not the documented detector-configuration field names. References/topics:

Administration > Detectors, Content Detectors, Path Detectors, Contain/Not Contain logic, AI Mesh detector contribution .

Question: 8

Which of the following are actions that can be performed from the Enterprise Search page? Select three.

- A. Revoking user permissions.
- B. Exporting reports.
- C. Moving risky files to a private folder.
- D. Manually changing the assigned risk.
- E. Manually verifying ML classification.

Answer: A, B, E

Explanation:

The correct selections are Revoking user permissions , Exporting reports , and Manually verifying ML classification . The Enterprise Search page is the primary file-level investigation view in Forcepoint DSPM. It lists scanned and cataloged files, allows filtering through standard filters or GQL, and provides operational actions against the returned results. Forcepoint states that Enterprise Search allows users to filter file data, save frequently used filters, customize columns, and generate meaningful reports. It also provides an EXPORT button that creates a CSV or JSON download of the filtered data.

Revoking permissions is also supported as a data-governance action. Forcepoint documents that administrators can view or modify file permissions and access rights from the file Actions menu, and supporting documentation identifies required permissions for revoke operations in Microsoft repositories.

Manual classification validation is explicitly available from the Enterprise Search hamburger menu. Forcepoint states that to adjust a file's machine-learning classification, the user selects Manually verify classification , modifies the ML-suggested classification, and saves the change. The incorrect choices are outside this specific Enterprise Search action set. Moving risky files to a private folder is not the standard named Enterprise Search action in this workflow, and assigned risk is not manually changed from the page. References/topics: Enterprise Search, Exporting Data, Permissions & Access Rights, Manual ML Classification Verification .

Question: 9

When Control Orchestration rules are triggered where can you find the events?

- A. Default dashboards
- B. Overviews
- C. Incidents
- D. Analytics

Answer: C

Explanation:

Triggered Controls Orchestration rule events are found under Incidents . In Forcepoint DSPM, Controls Orchestration rules are designed to identify data that requires attention by evaluating selected datasets, such as files, trustees, or agent activities, against rule conditions. When a rule condition is met, the result is operationalized as an incident so the security or governance team can review the matched data and determine the appropriate response.

Forcepoint's documentation states that each Controls Orchestration rule is "automatically added as a card in the Incidents tab," and selecting an incident card takes the administrator back to the related rule. It also explains that the Incidents section provides a top-down view of all orchestration rules and available match results. The documented navigation path is Policy Center > Incidents .

The other options are not the correct location for triggered orchestration events. Default dashboards and overviews provide summary visibility, but they are not the dedicated rule-event review workspace. Analytics supports broader investigation and reporting, but Controls Orchestration match results are reviewed through the Incidents workflow. References/topics: Policy Center, Controls Orchestration, Incidents, Rule Match Results, Enterprise Search Review .

Question: 10

Which of the following are steps in creating a data classification and handling policy? Select four.

- A. Specifying asset requirements.
- B. Identifying network traffic protocols.
- C. Incorporating industry-specific regulations.
- D. Defining classification levels.
- E. Outlining roles and responsibilities.

Answer: A, C, D, E

Explanation:

The correct selections are A, C, D, and E . A data classification and handling policy is a governance artifact that defines how data assets are categorized, owned, protected, reviewed, and aligned to legal or regulatory requirements. In Forcepoint DSPM, this sits within Policy Center and Compliance Hub , which are designed to support data classification, policy creation, security-control implementation, compliance, and risk reduction. Forcepoint states that Policy Center streamlines policy creation and prompts organizational representatives to provide information needed to build a governance framework aligned to organizational goals.

Specifying asset requirements maps to Data Mapping, where organizations define Data Asset Inventory fields and metadata such as retention period, business owner, regulatory scope, review status, and project name. Incorporating industry-specific regulations is required because departmental policy design must reflect obligations such as GDPR, HIPAA, and PCI DSS. Defining classification levels aligns to Taxonomy, where sensitivity levels such as Confidential, General Business, Public, and Highly Confidential are configured. Outlining roles and responsibilities aligns to assigning policy owners, department heads, representatives, and accountable stakeholders. Network traffic protocols are not a core step in creating a data classification and handling policy; they belong to network architecture or transport-control design, not data governance policy creation.

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/dspm-deploy-and-administer>