



SPLK-3001^{Q&As}

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/splk-3001.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

- A. Configure -> Incident Management -> Notable Event Statuses
- B. Configure -> Content Management -> Type: Correlation Search
- C. Configure -> Incident Management -> Incident Review Settings -> Event Management
- D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables>

QUESTION 2

Enterprise Security's dashboards primarily pull data from what type of knowledge object?

- A. Tstats
- B. KV Store
- C. Data models
- D. Dynamic lookups

Correct Answer: C

Reference: <https://docs.splunk.com/Splexicon:Knowledgeobject>

QUESTION 3

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

- A. Configure the add-ons according to their README or documentation.
- B. Disable the add-ons until they are ready to be used, then enable the add-ons.
- C. Nothing, there are no additional steps for add-ons.
- D. Configure the add-ons via the Content Management dashboard.

Correct Answer: A

QUESTION 4

Where is it possible to export content, such as correlation searches, from ES?



- A. Content exporter
- B. Configure -> Content Management
- C. Export content dashboard
- D. Settings Menu -> ES -> Export

Correct Answer: B

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export>

QUESTION 5

How is it possible to navigate to the list of currently-enabled ES correlation searches?

- A. Configure -> Correlation Searches -> Select Status "Enabled"
- B. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"
- C. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"
- D. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by "-Rule"

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches>

[SPLK-3001 Practice Test](#)

[SPLK-3001 Study Guide](#)

[SPLK-3001 Braindumps](#)