

Splunk Enterprise Security Certified Admin

Exam Description: The Splunk Enterprise Security (ES) Certified Admin exam is the final step towards completion of the Splunk ES Certified Admin certification. This app-specific certification exam is an 57-minute, 61-question assessment which evaluates a candidate's knowledge and skills in the installation, configuration, and management of Splunk Enterprise Security. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the [Splunk Enterprise System Administration](#) and [Splunk Enterprise Data Administration](#) courses or the [Splunk Cloud Administration](#) course, as well as the [Administering Splunk Enterprise Security](#) course, in order to be prepared for the certification exam.

The Administering Splunk Enterprise Security course focuses on Administrators who manage a Splunk Enterprise Security environment, including ES event processing and normalization, deployment requirements, technology add-ons, settings, risk analysis settings, threat intelligence and protocol intelligence configuration, and customizations.

The following content areas are general guidelines for the content to be included on the exam:

- Identifying normal ES use cases
- Examining deployment requirements for typical ES installs
- Knowing how to install ES and gather information for lookups
- Knowing the steps to setting up inputs using technology add-ons
- Creating custom correlation searches
- Configuring ES risk analysis, threat, and protocol intelligence
- Fine tuning ES settings and other customizations

The following topics are general guidelines for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 ES Introduction

5%

1.1 Overview of ES features and concepts

| | |
|---|------------|
| 2.0 Monitoring and Investigation | 10% |
| 2.1 Security posture | |
| 2.2 Incident review | |
| 2.3 Notable events management | |
| 2.4 Investigations | |
| 3.0 Security Intelligence | 5% |
| 3.1 Overview of security intel tools | |
| 4.0 Forensics, Glass Tables, and Navigation Control | 10% |
| 4.1 Explore forensics dashboards | |
| 4.2 Examine glass tables | |
| 4.3 Configure navigation and dashboard permissions | |
| 5.0 ES Deployment | 10% |
| 5.1 Identify deployment topologies | |
| 5.2 Examine the deployment checklist | |
| 5.3 Understand indexing strategy for ES | |
| 5.4 Understand ES Data Models | |
| 6.0 Installation and Configuration | 15% |
| 6.1 Prepare a Splunk environment for installation | |
| 6.2 Download and install ES on a search head | |
| 6.3 Understand ES Splunk user accounts and roles | |
| 6.4 Post-install configuration tasks | |
| 7.0 Validating ES Data | 10% |
| 7.1 Plan ES inputs | |
| 7.2 Configure technology add-ons | |
| 8.0 Custom Add-ons | 5% |
| 8.1 Design a new add-on for custom data | |
| 8.2 Use the Add-on Builder to build a new add-on | |
| 9.0 Tuning Correlation Searches | 10% |
| 9.1 Configure correlation search scheduling and sensitivity | |
| 9.2 Tune ES correlation searches | |

10.0 Creating Correlation Searches **10%**

- 10.1 Create a custom correlation search
- 10.2 Configuring adaptive responses
- 10.3 Search export/import

11.0 Lookups and Identity Management **5%**

- 11.1 Identify ES-specific lookups
- 11.2 Understand and configure lookup lists

12.0 Threat Intelligence Framework **5%**

- 12.1 Understand and configure threat intelligence
- 12.2 Configure user activity analysis