

# NSE Certification Program

## Exam Description

# FortiSIEM

## Certification

This exam is part of the Fortinet Certified Professional - Security Operations certification track. This certification validates your ability to secure networks and applications by deploying, managing, and monitoring Fortinet security operations products.

Visit the [Cybersecurity Certification](#) page for information about certification requirements.

## Exam

The *Fortinet NSE 5 - FortiSIEM 6.3* exam evaluates your knowledge, skills, and abilities to deploy, configure, administer, manage, and monitor FortiSIEM devices.

The exam tests a candidate's knowledge and skills related to basic to advanced configuration, day-to-day management of FortiSIEM devices, and integrating FortiSIEM into a network awareness infrastructure.

Once you pass the exam, you will receive the following exam badge:



## Audience

The *Fortinet NSE 5 - FortiSIEM 6.3* exam is intended security professionals responsible for the configuration and administration of FortiSIEM devices in an enterprise security infrastructure.

## Exam Details

|                 |   |
|-----------------|---|
| Exam name       | Fortinet NSE 5 - FortiSIEM 6.3  |
| Exam series     | NSE5_FSM-6.3  |
| Time allowed    | 60 minutes  |
| Exam questions  | 33 multiple-choice questions  |
| Scoring         | Pass or fail. A score report is available from your Pearson VUE account |
| Language        | English   |
| Product version | FortiSIEM 6.3   |

## Exam Topics

Successful candidates have applied knowledge and skills in the following areas and tasks:

- SIEM Concepts
  - Identify FortiSIEM architecture components
  - Identify deployment requirements
  - Identify event type classification
  - Perform system configuration and management tasks
  - Troubleshoot system configuration and deployment related issues
- FortiSIEM Operations
  - Discover devices on FortiSIEM
  - Build queries from search results and events
  - Tune data collection and notification processes
  - Deploy FortiSIEM agents
  - Troubleshoot discovery related issues
- FortiSIEM Analytics
  - Apply group by and data aggregation on search results
  - Use various reporting functions available on FortiSIEM
- Rules and Incidents
  - Identify various rule components
  - Configure rule sub-patterns, aggregation and group by
  - Manage incidents
  - Configure clear conditions for incidents
  - Configure notification policies



## Training Resources

The following resources are recommended for attaining the knowledge and skills that are covered on the exam. The recommended training is available as a foundation for exam preparation. In addition to training, you are strongly encouraged to have hands-on experience with the exam topics and objectives.

- *FCP - FortiSIEM 6.3* course and hands-on labs
- *FortiSIEM—User Guide 6.3*
- FortiSIEM 6.3 Installation Guides (various)
- FortiSIEM 6.3 Reference Manuals (various)

## Experience

Minimum of six months of hands-on experience with FortiSIEM devices.

## Exam Sample Questions

A set of sample questions is available from the Fortinet Training Institute. These questions represent the exam content in question type and content scope. However, the questions do not necessarily represent all the exam content, nor are they intended to assess your readiness to take the certification exam.

See the [Fortinet Training Institute](#) for the course that includes the sample questions.

## Examination Policies and Procedures

The Fortinet Training Institute recommends that you review the exam policies and procedures before you register for the exam. Access important information on the [Fortinet Training Institute Policies](#) page, and find answers to common questions on the [FAQ](#) page.

## Questions?

If you have more questions about the NSE Certification Program, contact us through the [Fortinet Training Institute Helpdesk](#) page.

