McAfee Enterprise Security Manager Administration 101

McAfee® Education Services Guided On-Demand Training

McAfee® Enterprise Security Manager—the heart of our security information and event management (SIEM) solution—provides near real-time visibility into the activity on all your systems, networks, databases, and applications. This enables you to detect, correlate, and remedy threats in minutes across your entire IT infrastructure. This course prepares McAfee Enterprise Security Manager engineers and analysts to understand, communicate, and use the features provided by McAfee Enterprise Security Manager. Through hands-on lab exercises, you will learn how to optimize the McAfee Enterprise Security Manager by using McAfee-recommended best practices and methodologies.

The McAfee® Enterprise Security Manager Administration 101 guided on-demand course from McAfee® Education Services offers you comprehensive and focused multimedia training from experienced instructors in a self-paced environment at your desk. The course delivers the same curriculum as the instructor-led training through virtual, on-demand coursework, recorded instructor presentations, use case scenarios from McAfee best practices and experiences, and hands-on lab exercises. You'll have email access to the instructor to get your questions answered.

Earn up to 32 CPEs after completing this course.*

* Student must self-report for CPE credits. We cannot guarantee any specific quantity, as it is up to the program or certification group to determine what they will or will not accept.

Audience

This course is aimed at McAfee Enterprise Security Manager users responsible for monitoring activity on systems, networks, databases, applications, and for configuration and management of the McAfee Enterprise Security Manager solution. Attendees should have a working knowledge of networking and system administration concepts, a good understanding of computer security concepts, and a general understanding of networking and application software.

Connect With Us

Agenda at a Glance

- Course Introduction
- Architecture Overview
- Devices and Settings
- McAfee Enterprise Security Manager Interface and Views
- Data Sources
- Working with McAfee® Enterprise Log Manager and McAfee® Enterprise Log Search
- Event Analysis
- Aggregation
- Watch Lists and Policy Editor
- Query Filters
- Rule Correlation
- Alarms
- Workflow and Analysis
- Reports
- System Maintenance and Troubleshooting
- Introduction to Use Case Design

Learning Objectives

McAfee Enterprise Security Manager Overview

Define McAfee Enterprise Security Manager and SIEM concepts, identify appliances and their features, and describe the McAfee Enterprise Security Manager solution component architecture.

Devices

Configure and customize receiver data sources and data source profiles.

McAfee Enterprise Log Manager and McAfee Enterprise Log Search

Configure McAfee Enterprise Log Manager settings, and mirror McAfee Enterprise Log Manager data storage.

McAfee Enterprise Security Manager Views

Effectively navigate the McAfee Enterprise Security Manager dashboard, and create custom McAfee Enterprise Security Manager data views.

Data Sources

Locate events and manage cases using a variety of data sources, assets, and enriched data.

Aggregation

Customize event and flow aggregation fields on a per-signature basis, and define the advantages and nuances associated with event and flow aggregation.

Policy Editor

Create, modify, and delete McAfee Enterprise Security Manager policies within the policy editor.

Recommended Pre-Work

It is recommended that students have a working knowledge of networking and system administration concepts.

Related Courses

- McAfee Enterprise Security Manager Administration 201 instructor-led course

Query Filters

Apply filters in views, create filter sets, use string normalization, and understand the basic syntax of regular expressions.

Correlation

Configure and deploy custom correlation rules within the correlation editor.

Watch Lists and Alarms

Create and configure watch lists and alarms.

Reports

Create and configure reports.

System Management

Perform routine maintenance on McAfee Enterprise Security Manager, including updates and clearing policy modifications and rule updates.

Troubleshooting

Perform troubleshooting steps associated with login issues, operating systems and browser-specific issues, hardware issues, and McAfee Enterprise McAfee Security Manager dashboard issues.

Use Case Design

Understand how the McAfee Enterprise Security Manager interface dashboards and views are used to identify specific events and incidents.

Learn More

To order, or for further information, please email **SecurityEducation@mcafee.com.**

6220 America Center Drive
San Jose, CA 95002
888 847 8766
www.mcafee.com