This course is aimed at McAfee customers acting as McAfee Enterprise Security Manager engineers who are responsible 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.
**COURSE DESCRIPTION**

**Agenda at a Glance**

- Course Introduction
- McAfee Enterprise Security Manager Overview
- Devices
- McAfee® Enterprise Log Manager and McAfee Enterprise Log Search
- McAfee Enterprise Security Manager Views
- Data Sources
- Aggregation
- McAfee® Enterprise Log Search
- Policy Editor
- Query Filters
- Correlation
- Watch Lists and Alarms
- Reports
- System Management
- Redundancy
- Troubleshooting
- Wrap-Up Scenario

**Recommended Pre-Work**

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

**Related Courses**

- McAfee Enterprise Security Manager for Engineers-II
- McAfee Enterprise Security Manager for Analysts-I
- McAfee Enterprise Security Manager for Analysts-II

**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**
Navigate and configure software updates, clustering, data sharing, replication, and asset sources and customize receiver system properties and communication settings.

**McAfee Enterprise Log Manager and McAfee Enterprise Log Search**
Navigate McAfee Enterprise Log Manager, configure settings, and mirror McAfee Enterprise Log Manager data storage.

**McAfee Enterprise Security Manager Views**
Effectively navigate the McAfee Enterprise Security Manager dashboard, configure and view the Scorecard, 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.

**McAfee Enterprise Log Search**
Configure McAfee Enterprise Log Search and search for specific events.
COURSE DESCRIPTION

Policy Editor
Create, modify, and delete McAfee Enterprise Security Manager policies within the Policy Editor and configure individual rules within the policy editor to meet your needs.

Query Filters
Create, configure, and apply filters in views and create filter sets.

Correlation
Define parsing and normalization processes within the correlation process and configure and deploy custom correlation rules within the policy 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.

Redundancy
Recall the McAfee Enterprise Security Manager clustering, McAfee® Receiver high availability and McAfee Enterprise Log Manager disaster recovery configuration techniques and design.

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

Wrap-Up Scenario
Use the McAfee Enterprise Security Manager interface dashboards and views to identify specific events and incidents in real-world examples.

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