COURSE DESCRIPTION

McAfee ePolicy Orchestrator Advanced Topics

McAfee® Education and Enablement Services Instructor-Led Training

The McAfee® ePolicy Orchestrator® Advanced Topics course from McAfee Education and Enablement Services provides in-depth training on the advanced capabilities of McAfee ePolicy Orchestrator (McAfee® ePO™) software. Through lecture, hands-on labs, and class discussions, you will learn how to use McAfee ePO advanced capabilities and practice using tools for upgrades and migrations, monitoring, maintenance and troubleshooting, and advanced policy configuration.

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.

Agenda at a Glance

Day 1:

- Course Introduction
- Installation and Cumulative Updater
- Migration
- Multiple McAfee ePO Server Features
- Monitoring and Optimizing McAfee ePO Performance
- Performance Optimizer

Day 2:

- McAfee® ePolicy Orchestrator Support Center
- Protection Workspace
- Logging and Reporting
- McAfee® Agent Logging and Reporting
- SNMP Reporting and Data Channel Troubleshooting
- Monitoring SQL

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with network and system security. A working knowledge of Microsoft Windows and network administration is recommended. A basic understanding of computer security concepts, internet services, viruses, and antivirus technologies are also recommended, along with six months experience using McAfee ePO software. Before taking this course, you should have completed the McAfee® ePO Administration course.

Connect With Us

Agenda at a Glance

Day 3:
- SQL Maintenance
- Web Application Programming Interface (API)
- McAfee Agent Relay
- McAfee® ePO Endpoint Deployment Kit (McAfee® EEDK)
- Disaster Recovery
- Advanced Queries

Day 4:
- Customizing Queries—Result Types and Charts
- Customizing Queries—Columns and Filtering
- Indicators of Compromise (IoCs)

Learning Objectives

Welcome

Become familiar with McAfee information and support resources and feedback mechanisms.

Installation

Identify installation requirements, recommendations, and best practices; identify and distinguish between the different deployment options for a new installation; install the McAfee ePO software.

Migration

Identify options for migrating the McAfee ePO server and database to new servers; perform post-migration tasks.

Multiple McAfee ePO Server Features

Configure rollup in a multiserver environment; register a server onto a local McAfee server, set up rollup server task, and set up rollup queries; move managed systems between servers using the Transfer System features; share policies in a multiserver environment.

Monitoring and Optimizing McAfee ePO Software Performance

Identify and utilize the best practices for monitoring and optimizing McAfee ePO software; explain how to use Performance Counters to monitor McAfee ePO server performance.

Performance Optimizer

Describe the key features and functionalities of Performance Optimizer; use the Performance Optimizer tool to troubleshoot a McAfee ePO software performance issue; explain how to monitor the database health using Performance Optimizer.

McAfee ePolicy Orchestrator Support Center

Describe the features and capabilities of McAfee ePO Support Center; explain how to use Support Center features to determine useful information regarding your McAfee ePO servers and installed products.

Recommended Pre-Work

- McAfee ePolicy Orchestrator Administration course
- Minimum of six months experience using McAfee ePO software

Related Courses

- McAfee ePolicy Orchestrator Administration
- McAfee® Endpoint Security Administration

COURSE DESCRIPTION

Protection Workspace

Describe the Protection Workspace feature; explain how to check in the Protection Workspace extension into McAfee ePO software; explain how to use Protection Workspace to monitor your environment.

Logging and Reporting

Describe and explain the functionality of the available McAfee ePO console log files; identify the commonly used agent, installation, and server log files; explain the basic troubleshooting for the agent, installation, and server log files; describe how to report on SNMP traps using McAfee ePO software.

McAfee Agent

Describe and explain the functionality of the available McAfee Agent log files; identify the commonly used agent, installation, and server log files; explain the basic troubleshooting for the agent, installation, and server log files. Explain how to use the Single System Troubleshooting tool that is provided with the McAfee Agent 5.6.1.

SNMP Reporting and Data Channel Troubleshooting

Describe how to report on SNMP traps from another server registered to your McAfee ePO server; describe how to troubleshoot the Data Channel.

Monitoring SQL

Define the strategies for basic SQL server design; identify best practices for maintaining SQL databases; explain how to manage database health using SQL tools and commands; define steps for identifying and managing large tables; use the McAfee ePO Purge Events Server task to reduce database size growth; explain how to run the main SQL queries used by Performance Optimizer; determine which SQL queries or services are utilizing the most resources in the SQL database.

SQL Maintenance

Define steps for backing up the McAfee ePO database in SQL; define steps for creating a maintenance plan for the McAfee ePO database.

McAfee ePO Web Application Program Interface (API)

Configure the McAfee ePO server for scripting; use Python scripting to extract data from SQL database; run advanced queries in scripts; explain how to get SIEM data from McAfee ePO software using the Web API.

McAfee Agent Relay

Identify a use-case list of where a McAfee Agent RelayServer can be useful; identify the port(s) that need to be open for using a RelayServer; identify how to configure the agent policy so that it can use the RelayServer; identify how to install a Windows and Linux agent to use RelayServer on a remote subnet.

McAfee ePO Endpoint Deployment Kit (McAfee EEDK)

Explain how to create and test McAfee ePO packages; explain how to get feedback in McAfee ePO CustomProps; identify how to use McAfee EEDK to deploy forensic tools; identify how to use McAfee EEDK to deploy Profiler for collection of performance reports; explain the process for McAfee ePO software migration and consolidation using the McAfee EEDK-packaged McAfee Agent.

Disaster Recovery

Describe the disaster recovery feature and how it works; explain how to use a server task to take a regular Snapshot; take a Snapshot from the Dashboard; identify the three main steps for manual disaster recovery; explain the procedures for manual disaster recovery.

Queries

Describe how to customize and design custom queries; explain best practices when designing queries.

Indicators of Compromise (IoCs)

Using McAfee ePO tools, find IoCs; describe how to analyze threat events; identify the actions for verifying the source of the infection; identify the steps for optimizing the security and performance of your systems; explain how to use the GetSusp tool to help locate and log undetected malware; explain how to use the GetClean tool to help minimize false-positive detections.

Learn More

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

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com