



# ePolicy Orchestrator Advanced Topics

Education Services Instructor-led Training

## Introduction

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

This course provides in-depth training on the advanced capabilities of ePolicy Orchestrator (ePO) software.

## DATASHEET

### Agenda At A Glance

#### Day 1

- Course Introduction
- Installation and Cumulative Updater
- Migration
- Multiple ePolicy Orchestrator server features
- Monitoring and optimizing ePolicy Orchestrator performance
- Performance Optimizer

#### Day 2

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

#### Day 3

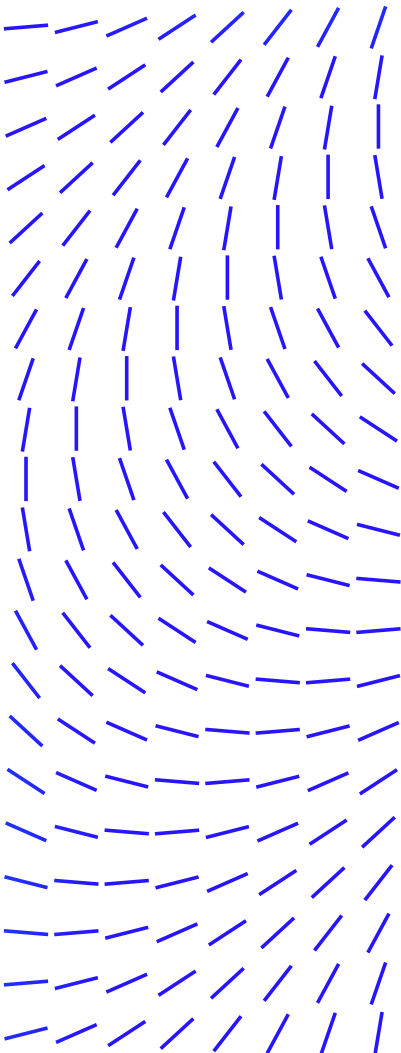
- SQL Maintenance
- Web Application Programming Interface (API)
- Agent Relay
- ePolicy Orchestrator Endpoint Deployment Kit (EEDK)
- Disaster Recovery
- Advanced Queries

#### Day 4

- Customizing Queries – Result Types and Charts
- Customizing Queries – Columns and Filtering
- Indicators of Compromise (IOC)

## 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 ePO. Before taking this course, you should have completed the ePO Administration course.



## DATASHEET

### Course Learning Objectives

#### Welcome

Become familiar with ePO 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 ePO software.

#### Migration

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

#### Multiple ePO server features

Configure rollup in a multi-server environment; register a server onto a local 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 multi-server environment.

#### Monitoring and optimizing ePO performance

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

#### Performance Optimizer

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

#### ePolicy Orchestrator Support Center

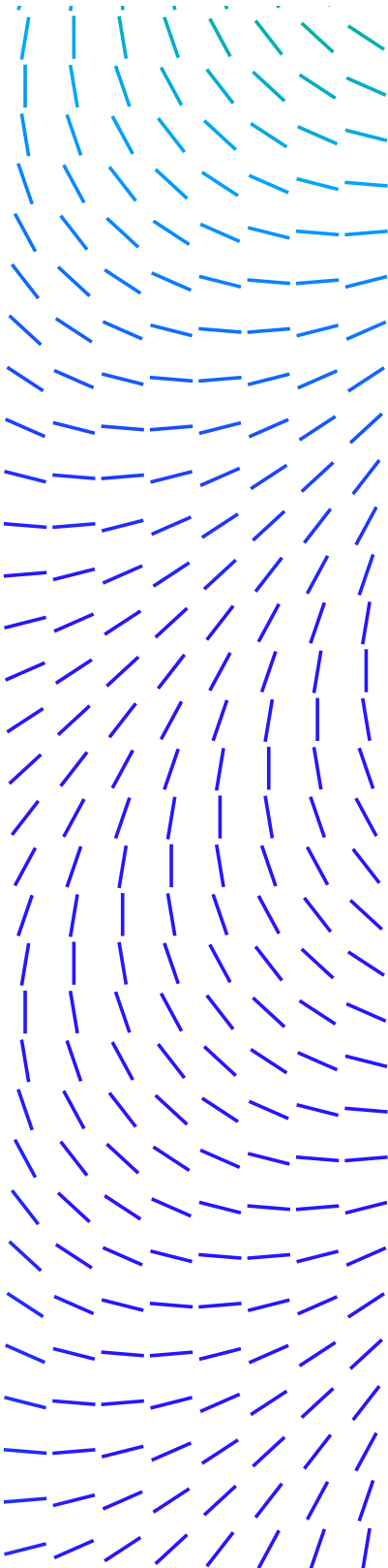
Describe the features and capabilities of ePO Support Center; explain how to use Support Center features to determine useful information regarding your McAfee ePO servers and installed products.

#### Protection Workspace

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

## Recommended Pre-Work

- ePolicy Orchestrator Administrator course
- Minimum of six months experience using ePO.



## DATASHEET

### Logging and reporting

Describe and explain the functionality of the available 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 ePO.

### 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.

### SNMP Reporting & 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 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 ePO database in SQL; define steps for creating a maintenance plan for the ePO database.

### ePO Web Application Program Interface (API)

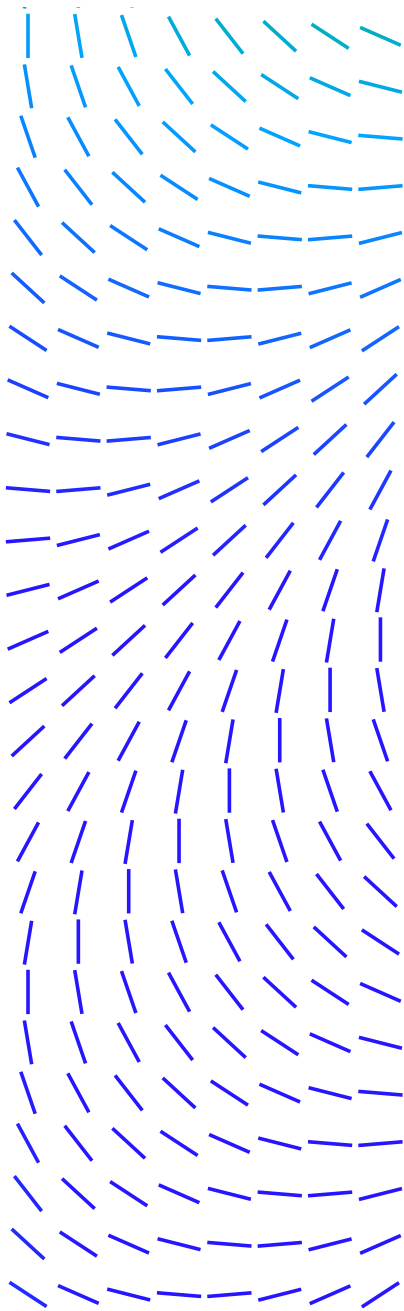
Configure the McAfee ePO server for scripting; use Python scripting to extract data from SQL database; run advanced queries in scripts; explain how to get SIEM data from ePO using the Web API.

### 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.

## Related Courses

- ePolicy Orchestrator Administration
- Endpoint Security Administration
- ePolicy Orchestrator Essentials



## DATASHEET

### ePO Endpoint Deployment Kit (EEDK)

Explain how to create and test ePO packages; explain how to get feedback in ePO CustomProps; identify how to use EEDK to deploy forensic tools; identify how to use EEDK to deploy Profiler for collection of performance reports; explain the process for ePO migration and consolidation using 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 the best practices when designing queries.

### Indicators of Compromise (IOC)

Using ePO tools, find Indicators of Compromise; 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.