TRELLIX

ePolicy Orchestrator – On-prem Advanced Topics
Instructor-Led Training

Highlights

Duration

4-days

Prerequisites

Students taking this course should have a working knowledge of Windows operating systems, system administration, and network technologies. Basic understanding of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies is recommended. Prior experience or working knowledge of ePolicy Orchestrator is also required.

How to Register

This course is available for purchase at https://trellix-training.netexam.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://trellix-training.netexam.com.

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

Learning Objectives

After completing this course, learners should be able to:

- Use ePO – On-prem advanced capabilities
- Use tools for ePO upgrades and migrations, monitoring, maintenance and troubleshooting, and advanced policy configuration

Who Should Attend

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with network and system security.

Course Outline

Day 1
- Welcome
- Installation and Cumulative Updater
- Migration
- Multiple ePO Server Features
- Monitoring and Optimizing ePO Performance
- ePO Support Center

Day 2:
- Protection Workspace
- Logging and Reporting
- Trellix Agent Logging and Reporting
- SNMP Reporting & Data Channel Troubleshooting
- Monitoring SQL
- SQL Maintenance

Day 3:
- Web Application Programming Interface (API)
- Trellix Agent Relay
- ePO Endpoint Deployment Kit (EEDK)
- Disaster Recovery
- Queries
- Customizing Queries – Result Types and Charts

Day 4:
- Customizing Queries – Columns and Filtering
- Indicators of Compromise (IOC)