Trellix ePolicy Orchestrator – On-prem 5.10 Advanced Topics

Education Services Instructor-led Training

Earn up to 16 CPEs after completing this course

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 On-prem Administration course.

Recommended Pre-Work

- Solid knowledge of Windows and system administration, network technologies
- Solid knowledge of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies
- Prior experience using Trellix ePolicy Orchestrator (ePO)

Related Courses

- Trellix ePolicy Orchestrator-On-prem Administration
- Trellix Endpoint Security Administration

Learn More

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

Our ePolicy Orchestrator - On-prem Advanced Topics course provides in-depth training on the advanced capabilities of 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

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 ePO.

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 ePO servers and installed products.

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

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.

Trellix Agent
Describe and explain the functionality of the available Trellix 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 Trellix Agent.

SNMP Reporting & Data Channel Troubleshooting
Describe how to report on SNMP traps from another server registered to your 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 man-aging large tables; use the ePO Purge Events Server task to reduce database size growth; 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 Programming Interface (AIP)
Configure the 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.

Trellix Agent Relay
Identify a use-case list of where a Trellix 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.

ePO Endpoint Deployment Kit (EEDK)
Explain how to create ad 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 Trellix 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.

Agenda at a Glance

Day 1:

- Course Introduction
- Installation and Cumulative Updater
- Migration
- Multiple ePolicy Orchestrator Server Features
- Monitoring and Optimizing ePolicy Orchestrator 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

Days 3:

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

Days 4:

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

Trellix

Visit Trellix.com to learn more.

042023-19