Trellix

DATASHEET

Trellix ePolicy Orchestrator

Education Services Instructor-led Training

Introduction

The Trellix ePolicy Orchestrator – On-prem Administration course from Education Services enables attendees to receive in-depth training on the benefits of the centralized management and deployment of products using ePolicy Orchestrator (ePO) software. Enabling administrators to fully understand the capabilities of their security solution not only reduces the risks of misconfiguration, but also ensures that an organization gets the maximum protection from installation.

Audience

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

Recommended Pre-Work

- Solid knowledge of Windows and system administration and network technologies
- Basic understanding of computer security and concepts

Related Courses

- Trellix Intelligent Sandbox Administration
- Trellix Data Loss Prevention Endpoint Administration
- Trellix Endpoint Security Administration
- Trellix ePolicy Orchestrator – On-prem Essentials
- Trellix Agent Essentials
- Trellix ePolicy Orchestrator Advanced Topics

Agenda at a Glance

Day 1:

- Welcome
- Security Solutions and ePO Overview
- Planning an ePO Deployment
- Installing ePO Software
- Managing Permissions Sets and Users
- Creating and Populating the System Tree
- Using the Tag Catalog

Day 2:

- Sorting the System Tree
- Trellix Agent
- System Information
- Client Tasks
- Managing Policies
- Policy and Client Task Approval

Day 3:

- Deploying Software for Managed Systems
- Repositories
- Product and Server Maintenance with Repositories
- Managing Dashboards and Monitors
- Working with Queries and Reports
- Automatic Responses and Notifications

Day 4:

- Database Maintenance and Server Utilities
- Disaster Recovery
- Agent Handlers
- Rogue System Detection
- Configuring Rogue System Detection

Learning Objectives

Welcome

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

Solution Solutions and ePO Overview

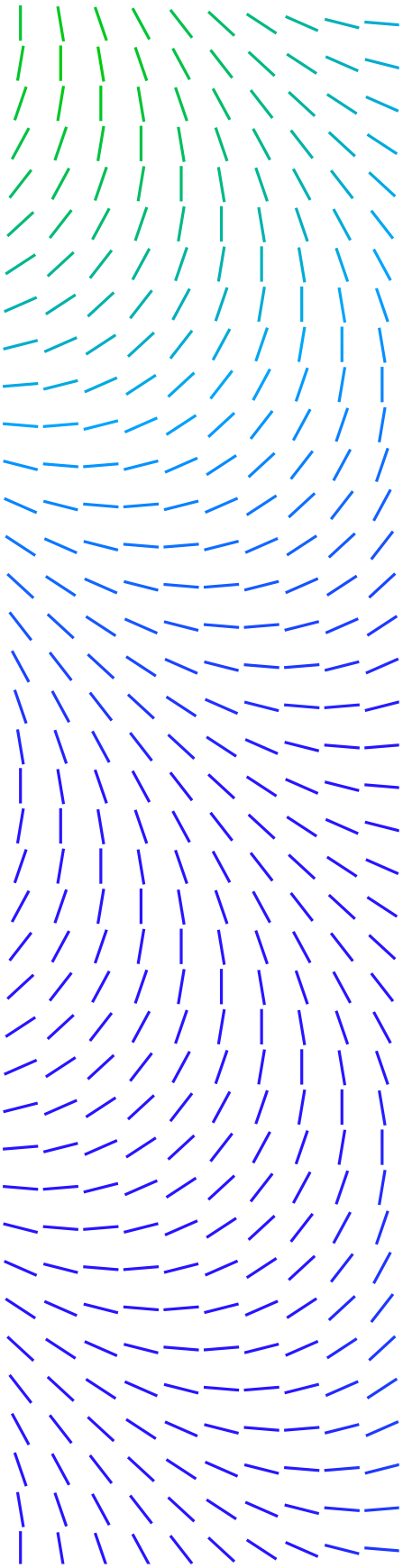
Become familiar with ePO information and support resources and feedback mechanisms.

Planning an ePO Deployment

Identify deployment considerations, describe deployment scenarios and solutions, identify ePO platform requirements, and discuss database sizing considerations.

Installing ePO Software

Identify installation requirements, recommendations, and best practices, distinguish between a new installation and a recovery installation, identify and distinguish between the different deployment options for a new installation, install ePO software; perform post-installation tasks, identify



configuration tools for the initial setup of the ePO software environment, and explain the process for upgrading ePO.

Managing Permission Sets and Users

Configure settings for personal settings, users, and permission sets; create a custom permission set, create users and assign permission sets, verify rights and access granted with permission sets, configure ePO and Active Directory user-based accounts, and verify rights and access granted with permission sets.

Creating and Populating the System Tree

Provide an overview of the ePO System Tree, use different methods for creating the System Tree, and describe the various methods of organizing the System Tree.

Using the Tag Catalog

Describe the purpose of tags and tag groups, learn the difference between tags without criteria (applied manually) and criteria-based tags (applied automatically and on-demand), how to create new tags, how to edit, delete and move tags between tag groups, and how to enable permissions for other administrative users.

Sorting the System Tree

Learn how to dynamically sort your machines into your ePO System Tree using a combination of system criteria, dynamically move machines into their appropriate group in your System Tree, and how to verify IP Integrity to ensure IP address sorting criteria does not overlap between different groups.

Trellix Agent

Define the Trellix Agent, explain its purpose and key characteristics and functions, and navigate the Agent interface.

System Information

View and interpret detailed information about your managed elements, customize your view, and view and customize System Monitors.

Client Tasks

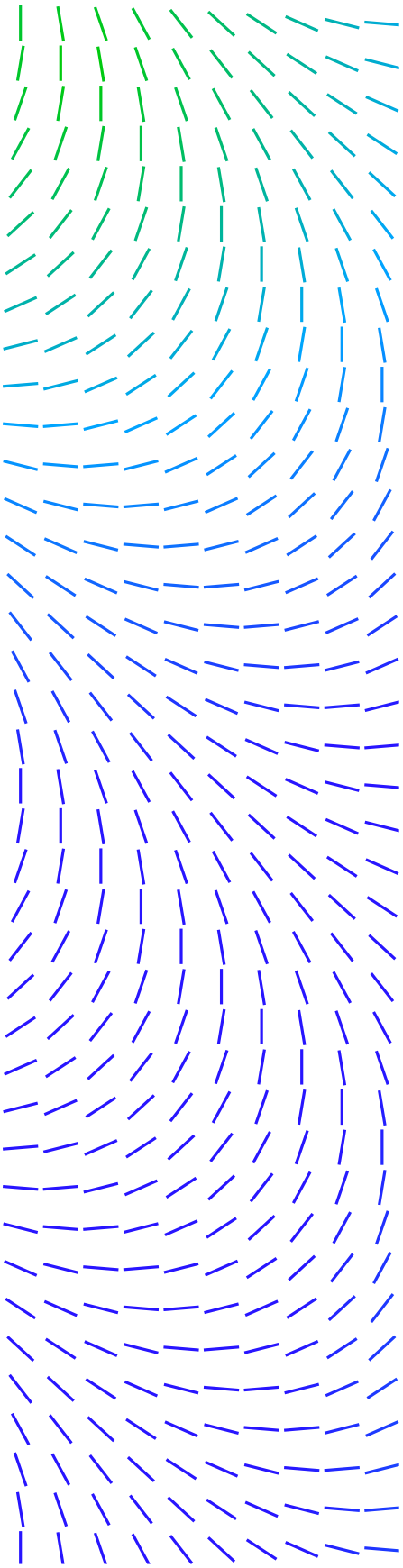
Describe the purpose of client tasks, communicate about client task concepts, access and navigate the Client Task Catalog, identify client task types, and add, duplicate, edit, schedule, and delete a client task.

Managing Policies

Describe the purpose of policies, create and edit policy objects, manage policy configuration and assignment, see policy inheritance in action, and enforce policy changes on client machines (endpoints).

Policy and Client Task Approval

Learn how to set up the approval process and how it works in ePolicy Orchestrator.



Deploying Software for Managed Systems

Identify different methods used to acquire required software components, explain how the Software Catalog works, install extensions and software components manually, check in required software components manually, distinguish between a Product Deployment Project and Client Task, and create a Product Deployment Project.

Repositories

Describe repository types and contents, explain the available branches for repositories; view the default repositories, create a source, fallback, distributed, SuperAgent, and unmanaged repository, and modify the repository contents and export the site list.

Product and Server Maintenance with Repositories

Update ePO-software-managed systems with scheduled or manual client tasks, configure the Global Updating feature to automatically update ePO-managed systems, manage ePO software repositories with server pull and replication tasks, and describe ways to troubleshoot client update task failures.

Managing Dashboards and Monitors

Identify the purpose of dashboards and monitors, as well as features and capabilities, identify default dashboards included with ePO software, access the Dashboards page, duplicate a dashboard, add a dashboard, and edit and assign dashboard permissions.

Working with Queries and Reports

Query the ePO database, use the Query Builder to create your own queries, explain how Multi-Server Roll-Up Reporting is performed, configure query permissions, configure Multi-Server Roll-Up Query Permissions, and export query data for viewing outside of ePO software.

Automatic Responses and Notifications

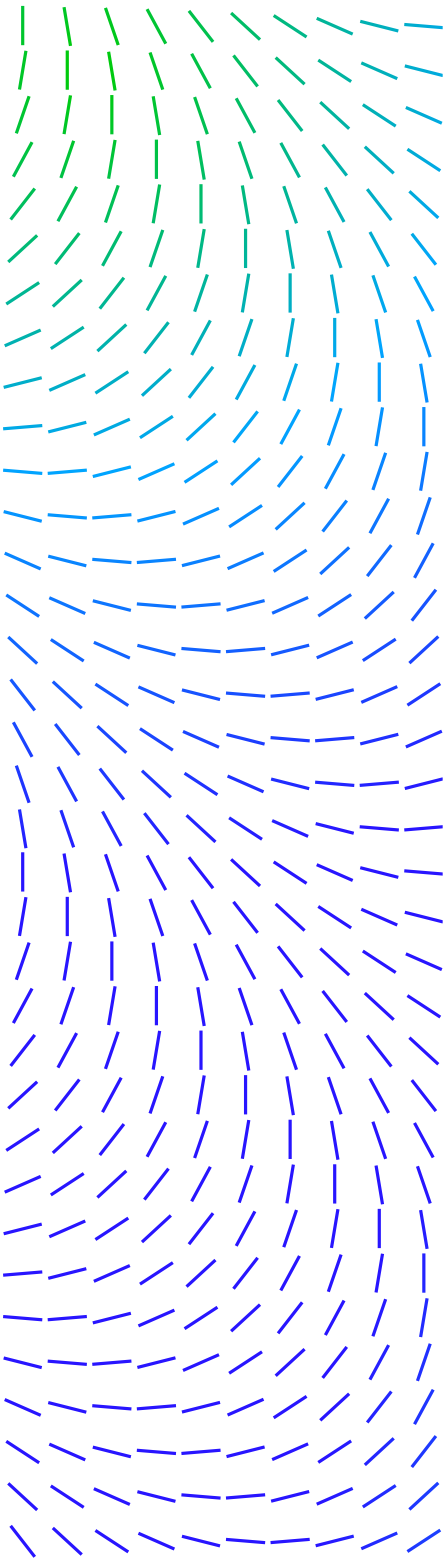
Use Automatic Response rules to create alerts and perform pre-determined actions, configure Automatic Responses, list the Permission Sets for Automatic Responses, and describe how to configure contacts for notifications.

Database Maintenance and Server Utilities

Identify maintenance tasks that should be performed on a regular basis, identify the primary SQL Server and ePO software tools you can use for maintenance, identify the recommended database recovery model, explain how to back up and purge data, identify ways to automate maintenance, and identify general server tasks.

Disaster Recovery

Describe the Disaster Recovery feature and how it works, use a Server Task for a Snapshot, take a Snapshot from the Dashboard, provide examples of Disaster



Recovery scenarios, explain the differences between an ePO software initial installation and a recovery installation, and describe best practices for Disaster Recovery.

Agent Handlers

Explain Agent Handler functionality and benefits, describe Agent Handler deployment scenarios and plan Agent Handler deployment, install and configure Agent Handlers, assign Trellix Agents to Agent Handlers and manage assignments, and create and manage Agent Handler groups.

Rogue System Detection

Explain the purpose of Rogue System Detection and how it works, determine the best place to install sensors on your network, examine sensor detection results and statistics, create policies for Rogue System Detection, install sensors onto machines in your network, and remove sensors from machines in your network, and view available Rogue System Detection queries.

Configuring Rogue System Detection

Configure Rogue System Sensor settings, permission sets and Automatic Responses for Rogue System Detection, monitor detected systems, and view available Rogue System Detection queries.

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

Trellix

022023-01