Trellix

DATASHEET

Application Control and Change Control Administration

Education Services Instructor-led Training

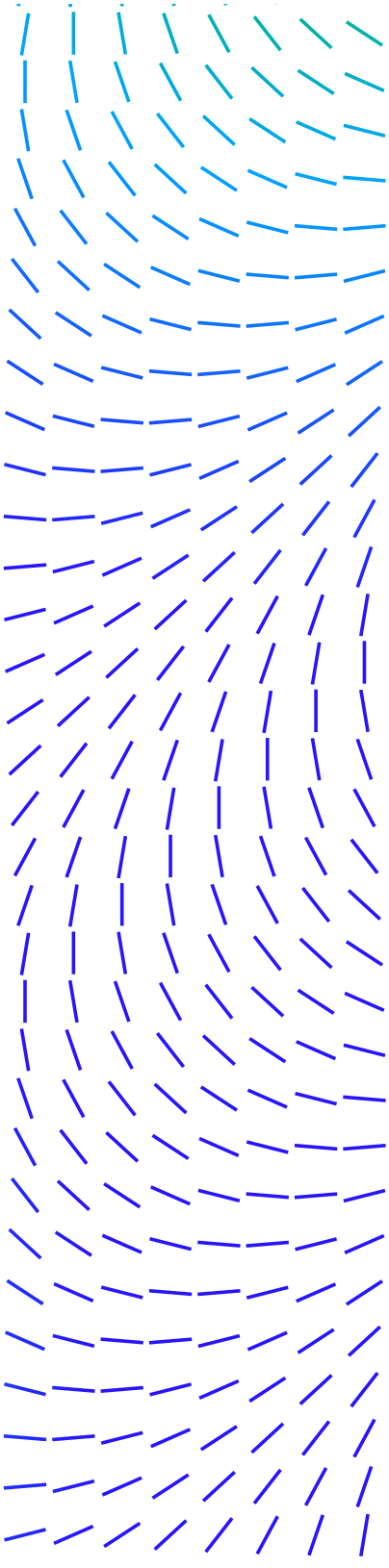
Introduction

The Application Control and Change Control Administration course from Education Services provides in-depth training on the tools you need to efficiently install, configure, operate, and troubleshoot issues relating to Application Control and Change Control to safeguard intellectual property and ensure compliance. The course details how this solution uses ePolicy Orchestrator (ePO) for centralized management. It also explains how to use Application Control for dynamic whitelisting to ensure that only trusted applications run on devices servers, and desktops and how to use Change Control to monitor and prevent changes to the file system, registry, and user accounts.

This course provides in-depth training on the tools you need to efficiently install, configure, operate, and troubleshoot issues relating to Application Control and Change Control to safeguard intellectual property and ensure compliance.

Audience

System administrators, security personnel, auditors, and/ or consultants concerned with system security should take this course.



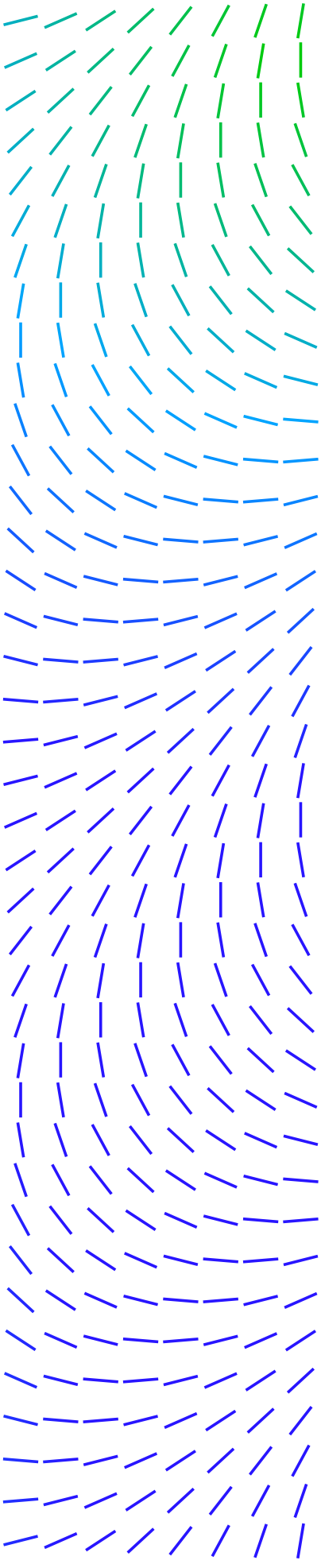
Course Goals

- Describe Application Control and Change Control solution.
- Plan Application Control and Change Control deployment.
- Install and configure Application Control and Change Control.
- Deploy and configure the Solidcore Client.
- Configure server tasks and permission sets.
- Create and manage policies and rules.
- Design the Application Control trust model.
- Manage the software inventory.
- Enable and configure Change Control.
- Configure Integrity Monitoring policies.
- Gather and analyze events and alerts.
- Create and interpret reports.
- Perform basic troubleshooting.
- Use Solidcore command line interface to perform endpoint administration.
- Identify best practices.
- Describes Inventory mode.
- Describes Common Platform Enumeration (CPE).
- Describes Trusted local group.
- Describes enhancements

Agenda At A Glance

Day 1

- Welcome
- ePolicy Orchestrator overview
- Application Control and Change Control overview
- Deployment and Extension Install



- Permission Sets
- Solidcore Client

Day 2

- Application Control Rule Groups and Rules
- Change Control Rule Groups and Rules
- Application Control Policies
- Application Control Trust Model
- Modify protected files

Day 3

- Application Control Inventory
- Change Control
- Integrity Monitoring
- Events and alerts
- Dashboards and Reporting

Day 4

- Troubleshooting
- Administration using the command line interface
- Recommended practices
- Case studies

Course Learning Objectives

Welcome

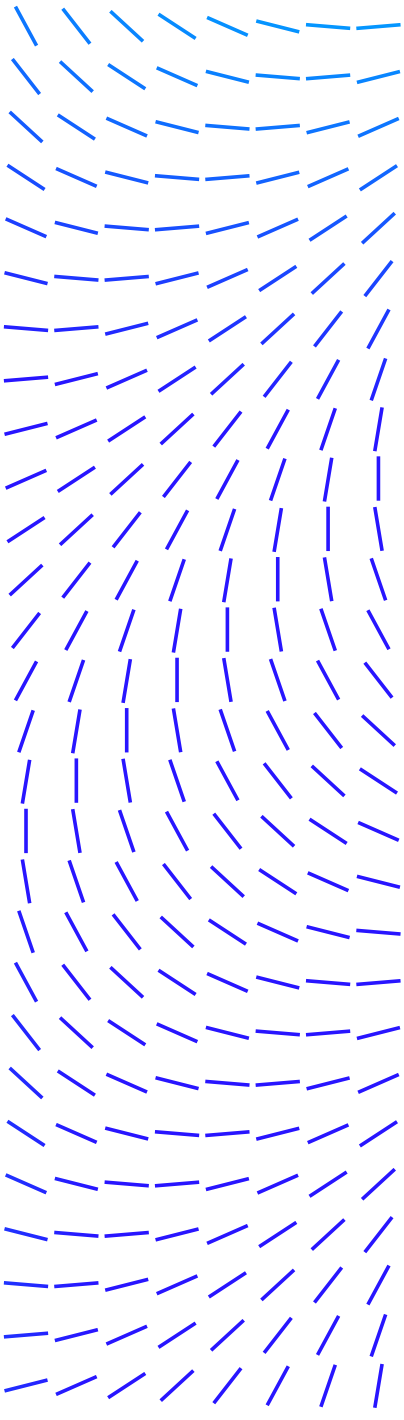
This first module provides an overview of course design, logistics, and helpful resources, as well as provides the opportunity for the instructor to learn about you and your training expectations.

McAfee ePolicy Orchestrator Overview

Describes ePO solutions basics, how ePO fits into the Security Connected model, ePO solution components and features, enhancements and changes for this ePO software release, and architecture.

Recommended Pre-Work

It is recommended that students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of internet services.



McAfee Application Control and Change Control Overview

Describe Application Control and Change Control components, features, and functionality.

Planning a Managed Deployment and Install ACC Extension

Describe the prerequisites and key parts of a deployment plan and identify solution considerations and pilot plan phases. How to add the Application Control and Change Control extension to the ePO server and verify installation.

Application Control and Change Control server tasks and permission sets

Identify default permissions sets included with ePO, Application Control, and Change Control and understand the product-specific server tasks created after deployment.

Solidcore Client

Describe how to enable and disable Solidcore Client tasks, describe end-user notifications, events, and approvals, and customize end-user notifications.

Rule groups and rules

Explain rule groups, rule group ownership, and rule groups permissions, configure and manage rule groups, and describe Application Control, Change Control, and Integrity Monitoring rule group tabs.

Application Control policies

Describe Application Control policies and their relationship to rule groups, define the role of the policy, and configure policies.

McAfee Application Control trust model

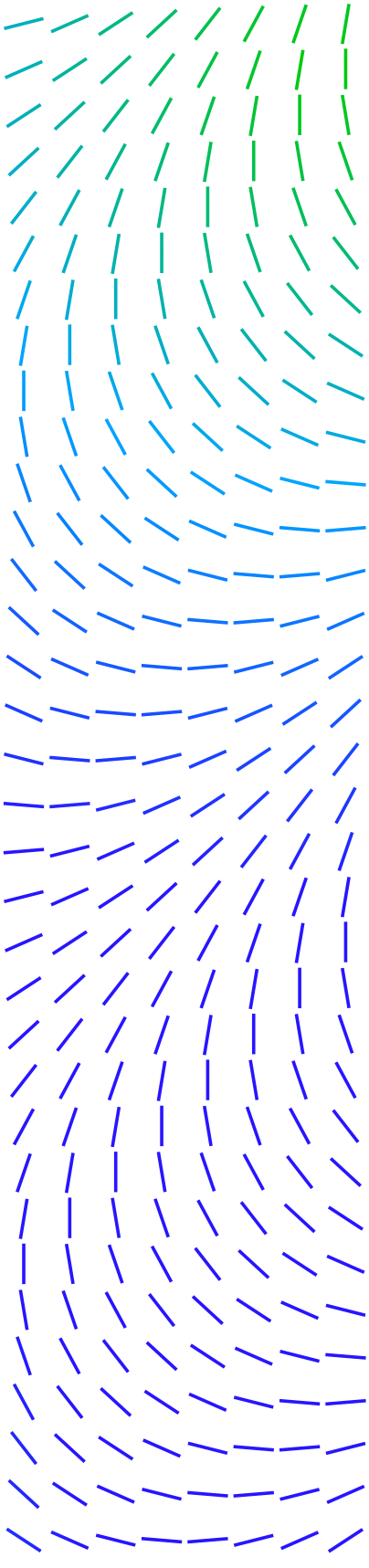
Understand the basics of whitelisting and design the Application Control trust model.

Modify protected files

Understand how to use Update mode and Observe mode and describe how to make rule modifications.

Application Control Inventory

Navigate the Inventory menus, describe how to fetch and manage an Inventory, and explain how to compare an Inventory.



DATASHEET

McAfee Change Control

Discuss how to use write protection and read protection in policies, define updaters and authorized users, and configure McAfee Change Control.

Integrity Monitoring

Configure Integrity Monitoring policies, reduce "noise" using and Advanced Exclusion Filter, and understand how to use content change tracking.

Events and alerts

Describe how Solidcore events are handled in ePO, understand when to use one-click exclusion, and configure Solidcore alerts in ePO.

Dashboards and Reporting

View and use Solidcore Dashboards and queries, and view Solidcore reports.

Troubleshooting

Identify Client versus ePO handling, locate log file and key resources, use troubleshooting tools, and troubleshoot feature implementation issues.

Administration using the command line interface

Use the command line interface to administer systems not connected to ePO.

Recommended practices

Identify best practices for initial setup, testing, policy creation and tuning, and maintenance.

Case studies

Create your own Application Control and Change Control policies without guidance and create a notification for violations of these policies.

Trellix